White Paper 4
Understanding Electrical Overstress - EOS

Industry Council on ESD Target Levels

August 2016

Revision 1.2

This document is available through various public domains as listed below:

The Industry Council on ESD
http://www.esdindustrycouncil.org/ic/en/

The Electrostatic Discharge Association
http://www.esda.org/

JEDEC – Under Publication JEP174
http://www.jedec.org/

Abstract

Damage signatures from Electrical Overstress (EOS) are the leading reported cause of returns in integrated circuits and systems that have failed during operation. Solutions to this problem are hindered by a prevailing misconception in the electronics industry that insufficient robustness to electrostatic discharge (ESD) is a primary cause of EOS. This document, White Paper 4, (WP) has been carefully compiled by the Industry Council on ESD Target Levels to foster a unified global understanding of what constitutes EOS and how EOS damage signatures can result from a wide variety of root causes.

The paper begins by outlining a brief history of EOS. It then presents the results of an industry-wide EOS survey. This survey gathered information on the types of EOS problems experienced by over 80 different companies, the relative importance of EOS to their overall business, and the methods assigned by these companies to address EOS issues. The survey provides a combined picture from which a more comprehensive definition of EOS can be made. The numerous categories and sub-categories of EOS root causes are explored in an attempt to understand how to create better specifications which will reduce their occurrence. In addition to the survey results, this paper studies many field returns with EOS damage signatures to establish the underlying root causes of damage and offers the respective identified solutions.

The survey and the case studies both show that successful failure analysis (FA) depends on careful communication between customer and supplier from the time a failure occurs until its cause has been discovered. Detailed investigation into manufacturing and handling processes is often necessary to accurately identify the root cause. This paper outlines a basic summery of the typical process flow for component electrical failure analysis.

The key point is that EOS issues can be mitigated when the proper understanding of IC design, factory and field environments, and system implementation is combined with effective communication across all these areas.

Purpose

This purpose of this white paper will be introduce a new perspective about EOS to the electronics industry. As failures exhibiting EOS damage are commonly experienced in the industry, and these severe overstress events are a factor in the damage of many products, the intent of the white paper is to clarify what EOS really is and how it can be mitigated once it is properly comprehended. It is very clear that EOS is predominantly a matter of what customers do with devices, and in which applications the semiconductor specifications are exceeded causing destruction of the device. This white paper will describe those phenomena and explain the most important facts so that the involved partners in the industry have the opportunity to understand and recognize helpful steps for analysis and avoidance of EOS events.

In view of the above, we define EOS in terms of its impact inside applications. We focus on exceedance of specifications but not on how an exact specification was originally created. We focus instead on when and how the specifications are exceeded to cause EOS damage.

It is intended that this document be disseminated throughout the semiconductor industry for the benefit of those persons whose positions are concerned with the real nature of EOS. It is intended to serve as a foundational reference document for existing and future technologies.

Additional Motivation

A key finding from the Council's investigation is that component level ESD specifications and robustness have at most a minimal role in leading to an EOS condition or causing returns that exhibit EOS damage. While relating ESD scenarios to EOS, the document explicitly emphasizes the non-correlation between EOS return rates and Component ESD Target Levels. This is fully in line with what has been established in the Industry Council's white papers published as JEDEC documents JEP155 and JEP157.

About the Industry Council on ESD Target Levels

The Council was formed in 2006 after several major U.S., European, and Asian semiconductor companies joined to determine and recommend ESD target levels. The Council now consists of representatives from active full member companies and numerous associate members from various support companies. The total membership represents IC suppliers, contract manufacturers (CMs), electronic system manufacturers, original equipment manufacturers (OEMs), ESD tester manufacturers, ESD consultants and ESD intellectual property (IP) companies.

Core Contributing Members	**Core Contributing Members**
Robert Ashton, ON Semiconductor	*Masaki Tanaka, Renesas Technology*
Fred Bahrenburg, Dell	*Christoph Thienel, Bosch*
Patrice Besse, Freescale	*Benjamin Van Camp, SOFICS*
Brett Carn, Intel Corporation	*Vesselin Vassilev, Novoroll*
Ann Concannon, Texas Instruments	*Jim Vinson, Intersil*
Jeff Dunnihoo, Pragma Design	*Scott Ward, Texas Instruments*
Charvaka Duvvury, Texas Instruments - Retired (Chairman) *cduvvury@gmail.com*	*Terry Welsher, Dangelmayer Associates*
David Eppes, AMD	*Joost Willemen, Infineon Technologies*
Reinhold Gärtner, Infineon Technologies	
Robert Gauthier, IBM	
Harald Gossner, Intel Corporation (Chairman) *harald.gossner@intel.com*	***Advisory Board***
LeoG Henry, ESD/TLP Consulting	*Agha Jahanzeb, Apple*
Satoshi Isofuku, Tokyo Electronics Trading	*Heiko Dudek, Cadence*
John Kinnear, IBM	*Stephen Frei, Technical University of Dortmund*
David Klein, Synaptics	*Ludger Kappius, Hella*
Hans Kunz, Texas Instruments	*Frederic Lefon, Valeo*
Timothy Maloney, Intel Corporation	*Christian Lippert, Audi*
Tom Meuse, Thermo Fisher Scientific	*Amit Abhay Mohabey, Tata Motors*
James Miller, Freescale Semiconductor	*Joseph Ney, GM*
Guido Notermans, NXP Semiconductors	*Patrice Pelissou, EADS*
Mototsugu Okushima, Renesas	*Wolfgang Pfaff, Bosch*
David Pommereneke, Missouri University of Science & Technology	*James Roberts, Continental*
M K Radhakrishnan, NanoRel Technical Consultants	*Marc Sevoz, EADS*
Wolfgang Reinprecht, AustriaMicroSystems	*Stephen Sibrel, Harman*
Alan Righter, Analog Devices	*Werner Storbeck, Volkswagen*
Theo Smedes, NXP Semiconductors	*John Timms, Continental*
Teruo Suzuki, Socionet	*Wolfgang Wilkening, Bosch*
Pasi Tamminen, Microsoft Corporation	*Rick Wong, Cisco*

Associate Members	**Associate Members**
Jon Barth, Barth Electronics	*Han-Gu Kim, Samsung*
Stephen Beebe, Global Foundries	*Marcus Koh, Everfeed*
Jonathan Brodsky, Texas Instruments	*Soon-Jae Kwon, Samsung*
Michael Chaine, Micron Technology	*Brian Langley , ORACLE*
Freon Chen, VIA Technologies	*Frederic Lafon, Valeo*
Ted Dangelmayer, Dangelmayer Associates	*Moon Lee, SemTech*
Ramon del Carmen, Amkor	*Markus Mergens, QPX*
Tom Diep, Texas Instruments	*Nate Peachey, Qorvo*
Stephanie Dournelle, ST Microelectronics	*Roger Peirce, Simco*
Melanie Etherton, Freescale Semiconductor	*Ghery Pettit, retired IEEE EMC Society*
Yasuhiro Fukuda, OKI Engineering	*Jeff Salisbury, Flextronics*
Howard Gan, SMIC	*Jay Skolnik, Skolnik-Tech*
Horst Gieser, FhG IZM	*Jeremy Smallwood, Electrostatic Solutions Inc.*
Mike Heaney, Amazon	*Jeremy Smith, Silicon Labs*
Masamitsu Honda, Impulse Physics Laboratory	*Arnold Steinman, Electronics Workshop*
Michael Hopkins, Amber Precision Instruments	*David E. Swenson, Affinity Static Control Consulting*
Kelvin Hsueh, UMC	*Nobuyuki Wakai, Toshiba*
Natarajan Mahadeva Iyer, Global Foundries	*Gene Worley, Qualcomm*
Larry Johnson, LSI Corporation	*Jon Williamson, IDT*
Marty Johnson, Texas Instruments	*Michael Wu, TSMC*
Peter de Jong, Synopsys	*MyoungJu.Yu, Amkor*
Jae-Hyok Ko, Samsung	
ChangSu Kim, Samsung	

Acknowledgments:

Editors:
Brett Carn, Intel Corporation
Hanna Klein

Authors:
Robert Ashton, ON Semiconductor
Fred Bahrenberg, Dell
Jeff Dunnihoo, Pragma Design
Charvaka Duvvury, Texas Instruments (Retired)
David Eppes, AMD
Reinhold Gärtner, Infineon Technologies
Harald Gossner, Intel Mobile Communications
Leo G Henry, ESD/TLP Consulting
John Kinnear, IBM
David Klein, Synaptics
Hans Kunz, Texas Instruments
Jean-Luc Lefebvre, Presto
Tim Maloney, Intel Corporation
Jim Miller, Freescale Semiconductor
M K Radhakrishnan, NanoRel Technical Consultants
Alan Righter, Analog Devices
Theo Smedes, NXP Semiconductors
Pasi Tamminen, Microsoft Corporation
Christoph Thienel, Bosch
Jim Vinson, Intersil
Terry Welsher, Dangelmayer Associates

The Industry Council would like to extend their heartfelt thanks to the ESD Association for their support in arranging meeting space for the Industry Council during the ESDA's regularly scheduled ESDA events.

Mission Statement

The Industry Council on ESD Target Levels was founded to review the ESD robustness requirements of modern IC products in order to allow safe handling and mounting in an ESD protected area. While accommodating both the capability of the manufacturing sites and the constraints posed by advanced process technologies on practical protection designs, the Council provides a consolidated recommendation for future ESD target levels as well as guidelines for various EOS and ESD topics. The Council Members and Associates promote these recommended targets and guidelines for adoption as company goals. Being an independent institution, the Council presents the results and supportive data to all interested standardization bodies.

Preface

This white paper has been written with the intent to provide a comprehensive understanding of what EOS is and is not, the importance of EOS to the industry, and what optimum measures can be taken to mitigate EOS damage to ICs, as well as products and systems. The wealth of material contained in this document should provide the industry with some often overlooked information as well as establish the notion that EOS is a complex phenomenon which requires thorough understanding on both the supplier side and the OEM side. This document should prove valuable to OEM and IC quality organizations, IC designers, failure analysis (FA) engineers, test engineers, customer interface, and system engineers. Our goal is that through this document more attention will be focused on properly addressing the often preventable failures exhibiting EOS damage. The chapters are organized to give as many technical details as possible to support the purpose explained in the abstract. The paper begins with an Executive Summary giving a high level message and ends with a list of frequently asked questions (FAQ) so that the reader can readily find critical information. These FAQs are intended to clear up misconceptions that commonly occur while interpreting EOS data.

Scope

The scope of this white paper is damage to integrated circuits and systems caused by electrical stress, the terms and definitions associated with electrical stress to these integrated circuits and systems and the mitigation of this electrical stress event as it applies to integrated circuits and systems.

Disclaimers

The Industry Council on ESD Target Levels is not affiliated with any standardization body and is not a working group associated with JEDEC, ESDA, JEITA, IEC, or AEC.

This document was compiled by recognized ESD experts from numerous semiconductor supplier companies, contract manufacturers and OEMs. The data represents information collected for the specific analysis presented here; no specific components or systems are identified.

The Industry Council, as well as the member organizations, while providing this information, do not assume any liability or obligations.

Table of Contents

Terms and Definitions

AC	alternating current
A/D	analog/digital
AEC	Automotive Electronics Council
AlCu	Aluminum Copper
AMR	absolute maximum rating
ANSI	American National Standards Institute
ASIC	application specific integrated circuit
ATE	automated test equipment
ATPG	automatic test program generation
BIST	built-in self-test
BJT	bipolar junction transistor
BTI	bias temperature instability
BVii	injection induced breakdown voltage
CAN	controller area network
CBE	charged board event
CBM	charged board model
CDE	cable discharge event
CDM	charged device model
CMOS	complimentary metal-oxide-semiconductor
CM	contract manufacturer
DC	direct current
DMOS	double-diffused metal-oxide-semiconductor
DSP	digital signal processing/processor
DRAM	dynamic random access memory
DUT	device under test
ECU	electronic control unit
ECL	emitter-coupled logic
EDX	energy dispersive X-ray
EIPD	electrically induced physical damage
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EMP	electromagnetic pulse
EOS	electrical overstress
ES	electrical stress
ESD	electrostatic discharge
ESDA	Electrostatic Discharge Association; ESD Association
ESDS	electrostatic discharge sensitive
ESREF	European Symposium on Reliability and Failure Analysis
FA	failure analysis
FAQ	frequently asked question
FEM	finite element model
FFR	failed failure rate
FIB	focused ion beam
FICDM	field induced charged device model
FICBE	field induced charged board event
FIT	failure-in-time

FMLB	first-mate-last-break
GND	negative voltage supply in digital logic, neutral voltage supply in analog logic
HBM	human body model
HCI	hot carrier injection
HMM	human metal model
HTOL	high temperature operating life
IC	integrated circuit
ICT	in-circuit test
IO	input/output
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPFA	International Symposium on the Physical and Failure Analysis of Integrated Circuits
IRPS	International Reliability Physics Symposium
ISTFA	International Symposium for Testing and Failure Analysis
ISO	International Organization of Standards
I-V	current/voltage
JEDEC	JEDEC Solid State Technology Association (formerly Joint Electronic Device Engineering Council)
JEITA	Japan Electronics and Information Technology Industries Association
JTAG	joint test action group
LC	inductor capacitor
LCT	liquid crystal thermography
LIN	local interconnect network
LIVA	light-induced voltage alteration
LSM	laser scanning microscopy
LU	latch-up
MCU	microprocessor control unit
MM	machine model
MOS	metal-oxide-semiconductor
MOSFET	metal-oxide-semiconductor field-effect transistor
NBTI	negative biased temperature instability
NiCr	nickel-chromium
NMOS	N-channel metal-oxide-semiconductor
NPN	negative-positive-negative (transistor)
OBIRCH	optical beam induced resistance change
OEM	original equipment manufacturer
PBL	powered bipolar latching
PCB	printed circuit board
PCBA	printed circuit board assembly
PMOS	P-channel metal-oxide-semiconductor
PNP	positive-negative-positive (transistor)
PPM	parts per million
PQFP	plastic quad flat pack
RC	resistor capacitor network
RF	radio frequency
SCR	semiconductor controlled rectifier; silicon controlled rectifier

SEM	scanning electron microscopy
SMD	surface mount device
SOA	safe operating area
SoC	system-on-chip
STM	standard test method
TC	timing circuit
TDDB	time dependent dielectric breakdown
TDR	time domain reflectometry
TEM	transmission electron microscopy
TIVA	thermally induced voltage alteration
TLP	transmission line pulse
TTL	transistor-transistor logic
TVS	transient voltage suppression
USB	universal serial bus
VDD	positive voltage supply
VFTLP	very fast transmission line pulse
VLSI	very large scale integration
VSS	negative voltage supply
VSWR	voltage standing wave ratio
W-B	Wunsch-Bell
WP	white paper

Definitions

electromagnetic interference (EMI): Electromagnetic emissions (radiated or conducted) which may cause harmful interference to communications services or other electronic devices.

ESD design window: The ESD protection design space for meeting a specific ESD target level while maintaining the required IO performance parameters (such as leakage, capacitance, noise, etc.) at each subsequent advanced technology node.

second-breakdown trigger current – (I_{t2}): The amount of current at the point in time when a transistor enters its second-breakdown region under ESD pulse conditions and is irreversibly damaged

Executive Summary

In this summary the Industry Council will address the most important electrical overstress (EOS) issues and conclusions of White Paper 4. Further details can be found in the various chapters of the document.

Traditional Perceptions of EOS

Through the years, a high incidence of failures exhibiting EOS damage has been reported in most market segments of electronics and related industries, such as the automotive industry. This damage has often been mislabeled as "EOS Failure", implying that these malfunctions are solely a result of a phenomenon or stress called EOS. Understanding EOS as a "stress" has led many customers to incorrectly assume a device experiencing EOS is "weak". This misperception has led to requests to "improve" a device in regards to EOS.

Another incorrect assumption has been that EOS can be avoided by making devices more ESD robust to both the human body model (HBM) and the charged device model (CDM). This misconception has been addressed in JEDEC publications JEP155 [1] and JEP157 [2] where it is convincingly shown that the incidence of EOS is independent of the level of HBM and CDM robustness.

Industry Council Worldwide Survey

In preparation for this white paper, the Industry Council conducted a worldwide survey of the electronics industry concerning EOS. Results confirmed the long held view that EOS is consistently one of the "high bars" on product failure Pareto charts. Looking at the EOS survey, respondents reported greater than 20% of total failures being EOS-related or 30% of total electrical failures being EOS-related, making EOS the largest bar on the Pareto chart of that responder's known causes of returns. One glaring revelation was the critical need for a better industry-wide understanding of EOS to address its issues.

Looking at the EOS survey further, misapplication (powered handling) stands out as the highest cause of EOS damage, with over 40% of respondents indicating EOS damage which occurred in the field as the most common location. Damage signatures associated with EOS often can involve package and silicon damage and are more extensive in a product than failure signatures resulting from events in the measurable ESD regimes. The main findings of the EOS Survey were:

1. **Powered Handling**: This stands out as the most widely reported root cause, involving a significant (over 20%) percentage of reported returns exhibiting EOS damage. Powered handling can include overvoltage, improper insertion, power supply sequencing, and incorrect biasing during use.

2. **Absolute Maximum Rating (AMR):** A number of returns exhibiting EOS damage were attributed to applied voltages exceeding the specified AMR voltage, indicating that incomplete or unclear maximum ratings may be an issue and that AMR characterization and improved AMR information on the datasheets is important to minimize the risk of EOS.

3. **ESD Related**: System level events, discharges from charged devices, and ESD controls in manufacturing which are not compliant with handling ESDS devices are additional root

causes for EOS damage. Charged board events (CBE) and cable discharge events (CDE) also contribute.

4. **Miscellaneous Causes**: There were other miscellaneous causes reported that ranged from weak printed circuit board (PCB) designs to mishandling.

New Definition of EOS Incorporating AMR and EIPD

It became clear to the Council during analysis of the survey, as well as gathering data on customer–supplier experiences with resolving EOS-related returns that a new way of visualizing the relationship of AMR to EOS is sorely needed in the industry. The Council proposes that the relationship between EOS and AMR may be illustrated in the manner indicated in Figure 1. Definition of AMR and its relationship to device stress, reliability impact and long and short term damage potential allows semiconductor manufacturers to clearly provide the maximum voltage / current / power limits. This enables system manufacturers to incorporate devices into their systems safely and ensure an operational environment that does not exceed those maximum limits. This is based on the following EOS definition:

An electrical device suffers an electrical overstress event when a maximum limit for either the voltage across, the current through, or power dissipated in the device is exceeded and causes immediate damage or malfunction, or latent damage resulting in an unpredictable reduction of its lifetime.

Critical to this definition is a clear understanding of what is meant by maximum limit. Chapter 3 further expands this definition by providing a practical interpretation of EOS in terms of AMR. Insight into the electrical aspects of AMR can be gained by examining the voltage ranges illustrated in Figure 1.

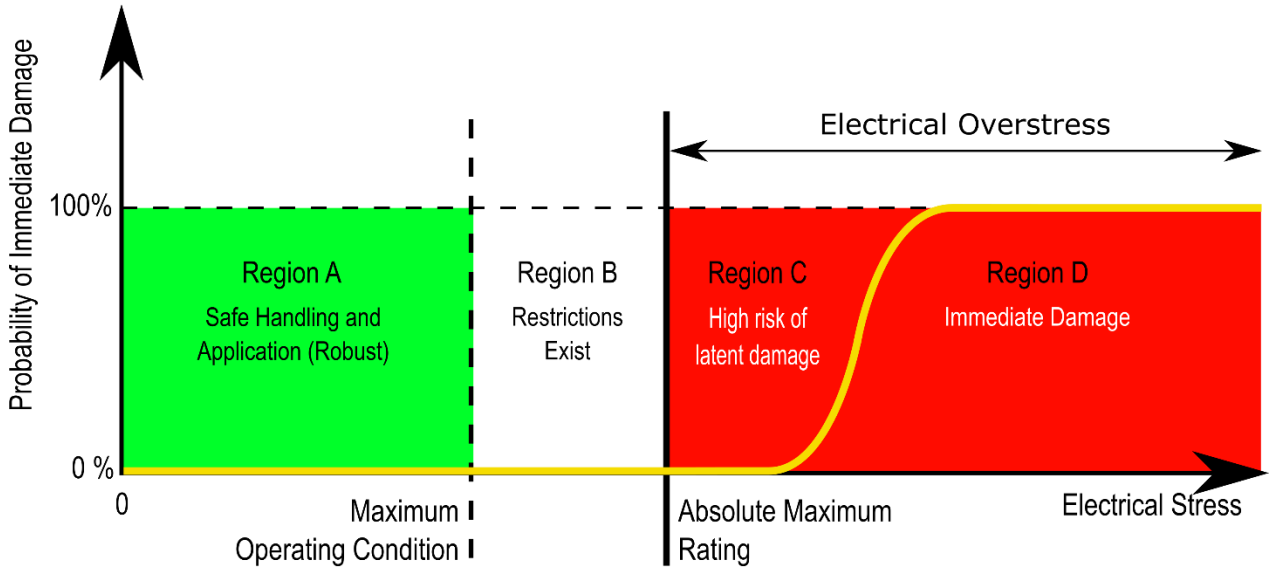


Figure 1: A graphical depiction of how Absolute Maximum Ratings should be interpreted. The yellow line is the number of components suffering immediate, catastrophic EOS damage

First, there is the safe operating area, a region of robust operation (region A). This is the region in which the manufacturer designed the device to operate. This is followed by a region in which operating restrictions exist (region B). In region B, the device is not guaranteed to function as specified, however the device is not expected to be physically damaged. Operating the device in region B for extended periods of time may also result in reliability issues. The upper limit of region B is the AMR. At and beyond the AMR the user should expect problems. Beyond the AMR are two regions of *electrical overstress* with either latent (region C) or immediate (region D) damage as a result of exceeding AMR. Note that the transition between latent damage and immediate damage is subject to normal process variations as illustrated by the yellow S curve. In order to properly evaluate the product reliability and robustness, it is important to understand that some qualification stresses, such as device level ESD and latch-up, are *expected* to run evaluations that will exceed AMR. For example, in the case of latch-up, this may be necessary in order to get significant current injection to assess latch-up robustness.

There are different methods a device manufacturer may use to determine AMR values. The manufacturer may pick very conservative AMR values not based on physical properties of the product. This results in a wide region C before the onset of immediate damage. Alternatively, the manufacturer may define the AMR values based on detailed circuit and technology understanding resulting in a more accurate prediction of the damage threshold. This can result in the near elimination of region C. Regardless of the method chosen, the manufacturer is solely responsible for defining the AMR. Further, an AMR is a function of stress duration and any single documented value will have a fixed time association. Consequently, a clear understanding of the AMR by a system manufacturer is necessary to ensure that the operating environment of the system is within the specified conditions and that the limits defined in the AMR are never exceeded. This is particularly important when the system is using the semiconductor device in new or unique configurations. In these special cases, communication between the supplier and system manufacturer *is absolutely necessary*, particularly if the AMR does not appear to cover a mode of operation the system manufacturer expects their system to experience.

Beyond this discussion of regions of operation where the AMR describes maximum electrical and environmental values of operation, there is controversy about whether it should also refer to ESD limits. As noted above, while recognizing that this definition of EOS focuses attention on the AMR, placing greater significance and expectations on its limits than may have been given in the past, each supplier has their own approach to setting the AMR values. With respect to ESD, several different approaches have been observed:

- Some suppliers do not include ESD limits as part of their AMR because testing to establish the ESD limits often does not have similar statistical data collected as is required for setting more traditional items such as voltage.
- Some suppliers do place ESD limits in their AMR definition as it is felt that this is part of the overall agreement that must be met between supplier and customer.
- Other suppliers have placed ESD limits in an AMR section did so for no other reason than it was the only place that it made sense to them.

Regardless of the approach taken, the supplier is *solely* responsible for deciding what parameters and limits are included in their product's AMR. Since this discussion on AMR could be a new interpretation of existing documentation, system manufacturers should be communicating with their

suppliers to verify that AMR information for any datasheet published prior to release of this white paper has appropriate meaning and that system manufacturers do not misinterpret the information as having a different meaning than the supplier originally intended.

This white paper also points out that failure analysis engineers are likely to assign, albeit some would say prematurely, the term EOS to any visible damage signature that appears to have been the result of excessive voltage or current. These assignments are often based on experience and may often be correct. However, after initial failure analysis, often times it is unclear as to whether a device has experienced EOS per this white paper's definition until further communication between supplier and customer has been carried out. The damage could be a violation of an AMR caused by incorrect biasing in the application, over voltage, induced latch-up conditions, extreme uncontrolled ESD, misorientation, or something else entirely. The damage may also have been due to a defect in an individual weak device, an improperly set AMR or an intrinsic weakness in the technology. To that extent, this white paper introduces the term "electrically induced physical damage" (EIPD) to represent the term that should be used by FA engineers when no clear communication has been completed with the customer as to possible root causes of the damage. The definition of EIPD is the following:

Damage to an integrated circuit due to electrical/thermal stress beyond the level which the materials could sustain. This would include melting of silicon, fusing of metal interconnects, thermal damage to package material, fusing of bond wires and other damage caused by excess current or voltage.

The term EIPD is used when it has not yet been determined if a unit experienced an EOS event by the definition of EOS above and elaborated on in Chapter 3. That conclusion can only be determined after the supplier and customer have worked together to arrive at potential root causes.

EOS Root Causes

As shown in the fishbone diagram of Figure 2, there are many categories and sub-categories for EOS root causes. The three main categories where EOS damage can occur are:

1) **powered handling**
2) **unpowered handling**
3) **switching / alternating current (AC) applications**

Each category can be traced to a specific sub-category shown as branches in the fishbone diagram of Figure 2. The sub-categories of Figure 2 are not meant to be an exhaustive list of root causes but an overview of some of the more common root causes.

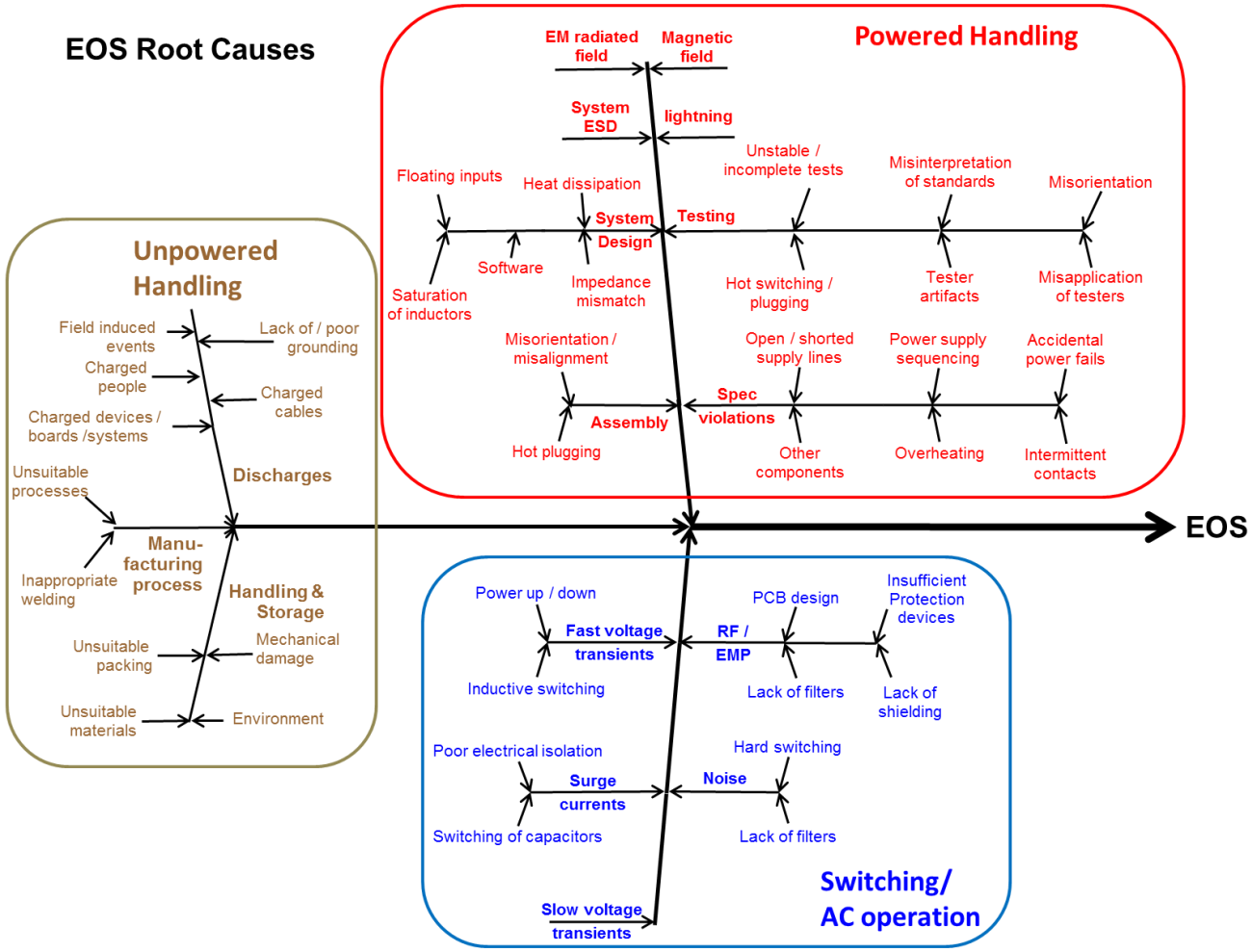


Figure 2: Fishbone Diagram Representing Different Root Causes Leading to EOS

Based on the EOS survey, the most common cause of EOS events is powered handling. Events may be related, for example, to overstress-induced phenomena when power is turned on, incorrect power supply sequencing, electromagnetic interference (EMI), or hot plugging. In addition, there are many system ESD events, especially during specification testing, which may result in unintended EOS damage. For responders showing a higher confidence level of finding a root cause of EOS damage (70 % to 100 %), a majority of those responders most often reported root causes which included hot plugging, overshoot / overvoltage, power surge, and misorientation being in their top 3, see Table 1 in Chapter 2. Clearly powered handling is an area where more focus is needed to address EOS damage.

In the unpowered branch, possible root causes include: an external charged source discharging into or through the device; the charged device/system being discharged; or the device/system being in an electrostatic field when the discharge has occurred. It should be noted that the root causes in unpowered handling are ESD-like in nature but may not be specifically related to the HBM or CDM testing performed as part of a product qualification. In fact, as the survey responses suggest, ESD represents a very small percentage of what constitutes EOS damage. Many manufacturers spend significant time auditing factories for ESD, thinking this will resolve all EOS events, when in

actuality, it will only address a small percentage of EOS related damage. Auditing a factory for EOS involves a much more in-depth look at power delivery systems and connection issues with significant focus on the powered handling root causes shown in Figure 2.

Typical root cause examples in the category of switching / AC operation are radio frequency (RF) coupling, spurious electromagnetic pulses (EMP) or poor PCB design, all of which may result in EOS damage. This category had the lowest reported incidence as root causes of EOS damage but this could be a result of the difficulty in properly assessing the environment for this category.

EOS Root Cause Diagnostics

When failed products are returned, proper failure analysis (FA) methods become crucial, but the success in determining *root cause* depends on the process flow used in this work. *Communication and cooperation* between customer and supplier *must* happen if the root cause is to be found. One challenge involves determining what can be classified as EOS and what should not be considered as EOS. The analysis itself can be lengthy as failure analysis times can range from days to months. Chapter 6 discusses the factors that play a critical role in the analysis time. The analysis can also be complex, involving tools from optical microscopy to acoustic microscopy to assess the component and many other advanced techniques including analysis of the system board characteristics. But this may only identify a *cause*. Coupling the device failure analysis with the product return signature and the use environment is critical to finding the *root cause*. While proper training and the tools available to FA engineers described in this paper are necessary, an FA engineer can only find the *cause* of the device damage (such as the identification of the damage signature and probable polarity / path of transients resulting in the damage), not the root cause of what created the EOS event as shown in Figure 2. Therefore, there must be a cooperative effort between supplier and customer to find the *root cause*. It should be noted that in some cases, such as in a singular damaged unit or if the use environment in which the damage occurred is unknown, it may not be possible to determine root cause.

EOS Case Studies and IC Designs

There are many EOS damage scenarios that can be avoided if the product field return causes are understood. White Paper 4 discusses these in detail and establishes some important conclusions on A) **Product EOS Returns**, B) **IC Technology / Design Issues**, and C) **Field and Factory Events**.

A) Case studies of product returns with EOS damage signatures were analyzed to determine a root cause. This allowed a reduction of EOS occurrences and demonstrated how appropriate solutions can be identified to meet customer needs. Some important conclusions are:

1. Failure analysis only provides a damage signature and probable path and does not reveal the true root cause.
2. Incorrect testing limits during qualification can lead to failures being falsely identified as EOS.
3. An EOS damage signature could be due to a broad list of root causes including, but not limited to; hot-plugging, ground bounces, supply switching, EMI transient surges, and process / product / system assembly issues.

B) Technology scaling and IC protection designs can also have some impact on EOS returns. A summary of these investigations reveal:

1. Today's advanced process technologies have not shown any obvious increase in return rates for products exhibiting EOS damage when compared to older, more robust technologies [1, 2]. It should be cautioned that further technology advances, with thinner gate dielectrics and novel transistor process technologies, will reduce breakdown voltages and continue to shrink design windows. This reduction in breakdown voltage will reduce AMRs and may subsequently begin to influence returns which exhibit EOS damage. In all cases, it will become even more critical to adhere to the AMR boundaries and maintain clear communication between supplier and customer.

2. As previously established, lowering ESD target levels for compatibility with technology scaling and circuit performance have no impact on EOS return rates.

3. However, IC ESD protection design styles and implementations can have an impact on EOS if careful adherence to AMR values is not addressed. A summary of the design styles and their impacts are summarized in Chapter 7.

C) Factory and field return analysis can provide lessons learned as listed below:

1. EOS damage can occur due to poor grounding methods and can easily be mitigated with established guidelines. A risk analysis often can avoid such problems.
2. Learning from field events is important. Many of the problems could be avoided if the supplier and the board designer communicate early in the product application development cycle having knowledge of possible root causes.
3. Automotive applications pose some of the most common risks. For example, hot plugging is a persistent problem in automotive electronics interconnection that can be mitigated by practicing the principle of first-mate-last-break.
4. EOS caused by ESD can be reduced by avoiding charging/discharging in manufacturing lines and implementing a balanced ESD protection approach.

EOS Mitigation and Communication

An important focus of this white paper is to convey the proper understanding of EOS, fostering communication between supplier and customer and reducing the number of returns exhibiting EOS damage in the industry. Useful customer communication methods are identified based on observed case studies and the expected influences from IC designs, production issues, field events, and application issues. Points to consider include:

1) Proper understanding of AMR
2) Realistic specifications of AMR and customer realization of its limits
3) Accurate determination of the location and possible causes of the damage and finding the true root cause event which created the damage
4) Understanding the use application and impacts to the IC's ESD protection design
5) Lessons learned from product returns from both manufacturing and the field

These are summarized to help the industry deal with returns exhibiting EOS damage.

Summary

This is the first known comprehensive document on EOS in electronics manufacturing and operations written to foster understanding of EOS, root cause determination for resolving EOS issues, and implementation of methods for EOS mitigation. A common language on EOS as documented here is the first significant step to help solve and mitigate EOS issues. IC suppliers, customers, applications engineers, and system builders alike should take part in understanding and solving EOS. Finally, customers and suppliers should treat all conditions for applications as a contract and agree that all unspecified conditions are not allowed. Education of these important aspects is the responsibility of all parties involved.

Outlook

For over four decades, EOS has been one of the top causes of returns for semiconductor devices and systems. The Industry Council has documented here an extensive study which enhances understanding of EOS and recommends many approaches to reduce EOS damage. This should be of great value in preventing EOS from becoming a catastrophic issue in the next generation of technologies involving even more consumer, medical, military, and automotive applications. It would be important to revisit the information presented here at a later date and conduct another industry wide survey to see how much impact this work has made. EOS *is* inherent in the application of electronic systems. Only through continuous learning and sharing of experiences can future risks be avoided.

References

[1] Industry Council on ESD Target Levels, "White Paper 1: A Case for Lowering Component Level HBM/MM ESD Specifications and Requirements," August 2007, at http://www.esda.org/IndustryCouncil.html or JEDEC publication JEP155, "Recommended ESD Target Levels for HBM/MM Qualification", www.jedec.org

[2] Industry Council on ESD Target Levels. "White Paper 2: A Case for Lowering Component Level CDM ESD Specifications and Requirements," Revision 2, April 2010, at http://www.esda.org/IndustryCouncil.html or JEDEC publication JEP157, "Recommended ESD-CDM Target Levels", www.jedec.org

Chapter 1: History of EOS

Leo G. Henry, ESD/TLP Consulting
Jeff Dunnihoo, Pragma Design
M K Radhakrishnan, NanoRel Technical Consultants
Jim Vinson, Intersil
Terry Welsher, Dangelmayer Associates

1.0 General Introduction to Historical References

In the 19th century, one of the first widespread applications of electro-mechanical systems with a well-known vulnerability to electrical overstress was the telegraph system. During storms, operators purposely ceased operations for fear of direct and indirect lightning strikes which could burn stations, melt wires and equipment and kill operators [1].

With the proliferation of vacuum tube communication equipment in the early 20th century, more complex component and system failure modes presented themselves. With the novelty of electronics in consumer applications, thermal and power supply robustness design issues competed with operator error and user repair problems. This formed the familiar basis for modern overload and overstress phenomenon.

Early radio repair (and kit construction) manuals of the 1920's and 30's included troubleshooting guides for finding melted grids and burned filaments on tubes, as well as procedures for determining failed open or shorted passive components when the hobbyist did not have even a voltmeter for debug.

The etymology of the term overstress implies a limit which is exceeded. This is synonymous with the term overload which was more generally used at the time to refer to any functional or permanent deviance from intended operation. Consider the following definitions from the Modern Dictionary of Electronics (1962) [2]:

OVERLOAD - 1. A load greater than that which an amplifier, other component, or a whole transmission system is designed to carry. It is characterized by waveform distortion or overheating. 2. In electronics, it is that quantity of power from an amplifier or other component or from a whole transmission system which is sufficient to produce unwanted waveform distortion.

OVERLOAD CAPACITY - The level of current, voltage, or power beyond which a device will be ruined. It is usually higher than the rated load capacity.

OVERLOAD LEVEL - The level at which a system, component, etc., ceases to operate satisfactorily and produces signal distortion, overheating, damage, etc.

At first glance, these would seem to be distinct from EOS, in that they pertain more to temporary functional failures or performance degradations. However, these passages elegantly define the resulting observations which are indicative of having exceeded maximum component limits. If we

consider a burned filament in a tube, or a shorted P-N junction in an integrated circuit, we can assume that the device will forever fail to perform with acceptable operational functionality.

Partial damage, such as a semiconductor with leakage, might be detected by signal distortion of a reference test pulse or level, overheating under normal loads, or visible physical damage. Thus the concept of permanent damage due to EOS can be found in the early definitions of overload which may or may not have created permanent damage, depending on the performance requirements.

Absolute maximum ratings (AMR) first appeared routinely in solid state datasheets in the late 1960's and early 70's. These limits are due to the unique process technologies of early emitter-coupled logic (ECL), transistor-transistor logic (TTL), and N-channel metal-oxide-semiconductor (NMOS) which alerted the designers to power supply and interface level limits at a time when signaling voltages and polarities were not strictly defined and constrained by unique interface designs (such as RS-232, IEEE-488, etc.)

Generally, while input signals could cause problems in some circuitry, AMR's tended to convey a guarantee by the component supplier that if the thermal and voltage envelope limits were not exceeded, the component would never be permanently damaged or degraded and would remain completely within all other electrical performance specifications.

Exceeding the AMR for any period of time did not guarantee permanent damage, and indeed the ratings were often very conservative or “sandbagged” with wide guard bands because it was often difficult for designers to accurately gauge the robustness limits of a new technology.

1.1 Outline of History of Relevant Professional Societies

This historical note by Colvin [3] covers the origin of many EOS related professional societies:

"Published papers for Failure Analysis date back to 1954 for the Annual Symposium on Reliability and back to 1963 for the International Reliability Physics Symposium (IRPS). Another familiar resource to the failure analyst in the USA is the Symposium for Testing and Failure Analysis (ISTFA). ISTFA proceedings were originally known as ATFA (Advanced Techniques in Failure Analysis) and date back to 1974. The Microelectronic Failure Analysis Desk Reference (1996-2012) is an important companion to the ISTFA Workshops. IPFA (International Symposium on the Physical and Failure Analysis of Integrated Circuits) is another resource of information. The conference for IPFA has been held annually in Singapore for the last 6 years *(ED NOTE: since 1987)*. ESREF is a European forum for reliability of electron devices, failure physics and analysis. ESREF held its first symposium in 1990. The annual EOS/ESD Symposium started in 1979 in the US. One of the goals being to elevate the awareness to the destructive nature of EOS and ESD to electronic components. Additional resources of information are the Journal of Electrostatics, an Elsevier publication, ESA (Electrostatics Society of America), and IEJ (Institute of Electrostatics Japan)".

1.2 EOS – A Brief History

Two of the earliest researchers were Wunsch-Bell [4], who did not mention EOS by name but whose physical modeling implied a path to melting at high temperatures for semiconductor components. The time dependent Wunsch-Bell equation generally defined as $P/A = f(t^x)$ also shows that the power per unit junction area varies with pulse width, and is actually a thermal diffusion equation which depends on thermal conductivity and the product of density and specific heat. This model characterizes a component's failure power threshold versus an input pulse duration (time dependent pulse width). A plot of the device behavior shows 3 regions: a short pulse width (<0.1 µs) ESD region, a longer pulse width (0.01 – 20 µs) Wunsch-Bell region, and a very long pulse width (> 20 µs) flat region. This is the region which leads to melting, because the thermal conductivity and the density-specific heat product are both temperature dependent properties of the semiconductor material, and so this flat pulse width region is directly related to EOS type failures, as a result of high heating with time in addition to pulse width.

Additionally, some early mentions of the word overstress appears to be in 1971 [5], when Smith and Shumka were analyzing complimentary metal-oxide-semiconductor (CMOS) microcircuits and silicon devices. They reported that up to 29 % failed due to external overstress; unfortunately a detailed FA of these failures was not included. In 1979 [6], Rutherford and several others reported on the electrical overstress of digital bipolar microcircuits and silicon devices claiming that 60-75 % were EOS damage. Some used charged capacitors (up to 0.01 µF) as the input stress. Lee [7] attempted to interpret the EOS damage in power transistors and semiconductors. Melted bond wires, fused or alloyed metallization all fell under the category of EOS damage.

From 1983 to 1985, several authors, Lee [8], Middendorf [9], and May [10] reported the EOS damage from power circuits to power transistors. They used the terms *melted metal*, *dissolved metal*, *melt-through* and *burnt metal* in their description for EOS damage, but there was no mention of the bond wires. The use of the combined terms EOS/ESD is significant, where the combined term is used to mean EOS and/or ESD, i.e. EOS alone, ESD alone or both if the diagnosis is uncertain. However, the authors pointed out that the use of the shorter duration pulse distinguished between the ESD damage and the longer pulse EOS damage, in most cases.

In 1988 [11], Lee conducted simulation and characterization of EOS damage in metal-oxide-semiconductor field effect transistor (MOSFET) transistors and ICs by capacitive discharge. Here, Lee used much larger capacitors (200 µF to 4500 µF) to dump more energy into the device. Lee reported that the large metal melt-through also obliterated the ESD protection circuits. The wire bonds were also damaged. Using the lower capacitance (up to 200 pF) resulted instead in ESD damage between the source and drain in the ESD circuits. Hence, differentiating between EOS and ESD damage was of primary importance early on.

In 1989, Richardson Jr. [12] described an overvoltage stress test in TTL electronics, which resulted in melted metal, open metallization, melted input transistors, and damaged input protection diodes. A curve tracer was used as the voltage simulator, and all voltages were greater than the rated maximum voltages for the TTLs. The failures were referred to as electrical damage. The same year, Kiefer [13] studied the damage in high-speed CMOS gate arrays using the machine model (MM) as the simulator (in order to produce more power) and referring to the process as an EOS stress. This resulted in the usual fused/melted metal, all damage being visible with a low magnification microscope. At lower machine model (MM) voltages, the damage was not immediately visible, but

on removal of topside glass/oxide and the metal below, the damage could be seen in the oxide below the drain-to-source contacts. These were referred to as ESD melt filaments failures. These authors simulated an EOS stress after first ESD stressing the devices. They called this an "ESD/EOS" stress, meaning ESD stress followed by an EOS stress. The damage seen was fused metal plus protrusions of poly-silicon melt filaments in the contacts, and also between the contacts. These authors were attempting to show the difference between EOS damage and ESD damage.

Also in 1989, two authors (Willis [14] and Kitamura [15]) discussed locating EOS/ESD failures without explaining why they used the combined terms (EOS/ESD). They reported the following long list of failures: damaged/degraded junctions, blown open and punched through contacts, ruptured dielectrics, gate oxide pin holes, gate edge pinholes, aluminum melting, fused open aluminum metal, thermal damage of diffusion resistors, and melted silicon. They only used two electrical stress types, HBM and transmission line pulse (TLP), and labeled some figures EOS, and some ESD, with no clear discussion or clarification as to which failure belongs to the two different stresses.

Launer [16] related discoloration to EOS damage in 1990 when he presented EOS damage data after electrically overstressing passivated nickel-chromium (NiCr) resistors using two different pulse sources (a HBM 150 ns pulse width and a 200 ns to 120 µs square pulse). He referred to HBM as an alternating current (AC) source of adiabatic EOS, resulting in discolored NiCr resistors because there was no significant heat beyond the oxide. He referred to the square pulse as a direct current (DC) source with its long pulse width, which also caused EOS damage (including the discoloration) in the NiCr resistors. No explanation was given in the report as to why these two different events resulted in the same EOS type damage.

May, [17] in the same year (1990), presented and discussed the EOS discoloration concept, but applied it to the metallization using pulse widths of 10 µs, 120 µs, through to DC. The author concluded that the lateral thermal diffusivity occurs in the metallization, and therefore across the whole device.

Between 1991 and 1994, several authors, Wilson [18], Schani [19], Glacet [20], and Henry [21] demonstrated that EOS damage could be produced from either negative/positive step stress pulses, overvoltage/overcurrent stressing, from IC life test, and IC burn-in attributing one mechanism to the process-induced metal stress relief during the IC life test and/or burn-in test. This EOS simulation allowed the authors to speculate as to how to differentiate between EOS and ESD type damage. Then, in 1998, Henry and Mazur [22] in their paper "Basic Physics in Color-Coded EOS Failures" were able to do just that by applying some physics principles to the process. The visible EOS damage was the same as that seen by earlier authors: die surface burnt, fused metal, etc.

Most of the previously mentioned authors reported that EOS damage was optically visible at very low magnification - open metallization, fused metal, burnt/discolored metal, melted metal, fused open metal, package distortion/blistering, and melted sockets (on the board). One author used the non-destructive acoustic microscopy method to externally view the EOS damage inside the package. The package compound was shown to be thermally degraded. It showed internal delamination (die interface-die attach), voids, the aluminum wires were fused or burnt and had molding compound on them, die cracks, burnt/carbonized plastic, and package cracks under the die pad. They also reported the electrical signatures as shorts, opens, high leakage, and high resistance.

In 1995, Lisenker [23], working on a CMOS very large scale integration (VLSI) product, used the combined term ESD/EOS to mean ESD stress, followed by EOS stress to simulate the observed failures. He suggested that the metal burn-out occurred after the gate oxide punch-through (or juncture failure) occurred, creating a short which drew enough current in a powered device to melt the metal stripe. Hence the use of the combined term ESD/EOS. He used burn-in, a process of operating the device under certain electrical and thermal stress conditions which accelerates the life of the device and removes poor quality devices. Several other authors in the same year [24], 1995, showed EOS damage in insulated-gate bipolar transistor modules (each module contained several devices). The damage included burnt wires, melted wires, melting pits in bond pads, and melted material penetrated deep in the silicon chip. They used a square pulse frequency test (high voltage 50 Hz -12 kHz cycles 600 V-1300 V) through a charging capacitor and inductor.

In 1997, Milburn & Parekh [25] reported that the EOS damage (melted/open metal) was precipitated by excessive voltage or power generating a high current over a period of time, and in 1998 Vinson [26] studied the aluminum interconnect response to EOS, calling EOS the stress, instead of the failure, and reporting that EOS is the event causing the failure, and the aluminum film responded to the EOS event. They concluded that Joule heating caused failure as a result of excessive currents due to overvoltage from a power surge, inductive kickback from an inductive load, or application of a voltage to an output pin in the nanosecond to second range. They provided the following definition of EOS: "a class of failure from an applied stimulus condition exceeding the normal operation of the circuit". Yet some authors referred to the failure as aluminum EOS, or EOS damage or EOS of aluminum lines—all interchangeably.

In 2001, Wang [27] described EOS damage as a result of over-current or over-voltage events ranging from microseconds to milliseconds. The author reported that EOS causes uncontrollable overheating (thermally induced failures) which leads to electromigration failure, intermetallic compound formation, and delamination on die surface. Vinson [28] also saw EOS damage, but the cause of the EOS was an excessive electrical stimulus (V or I) applied to the unit resulting in the damage. EOS then is an event that occurs at a point in time, triggering the failure. It is not a wearout mechanism that degrades with time, but the failure is quite visible, and in some cases the metal from the contact migrates into the silicon shorting out the junction (damaged junction).

In 2003, Korchnoy [29] showed that the silicon substrate and diffusion layers can be affected by ESD in such a way that the damage extends up though the interlayer dielectric to the metallization causing it to melt both at the contacts and the metallization because of the excessive current flow. He called these ESD/EOS failures, i.e. ESD induced EOS damage.

1.3 Transition to Present

In the period between the earliest, most elementary electrical circuitry overloads and the more recent academic and industrial analysis, the body of knowledge, terms and definitions have grown dramatically. EOS damage has been categorized by early researchers based on the physical results to try to determine the type of event, energy content, and duration of the event to help identify the source. Papers defining a method to characterize devices for EOS robustness were not always present. Also, most did not include physical modeling of EOS in the semiconductor devices, but there were some papers which attempted to describe how to improve the safe operating area (SOA)

of transistors, SOA refers to the maximum voltage and current that a transistor can sustain without damage under specific conditions.

While the mechanisms may be related or even identical, often the definitions and terms used coherently within the scope of one paper or author may be confusing or even conflicting when compared to other sources. As Alfred Korzybski observed, it is important in any semantic system to index and date the terms used whenever the same word may be mapped by different authors and readers to different meanings at different times. The underlying physics of the phenomena may remain timeless and universal, but the labeling and classification may have been inconsistent.

The balance of this document investigates these issues in more detail and tries to add clarity to the use of the terms and definitions, aided with the benefit of the historical literature amassed so far.

References

[1] Modern practice of the electric telegraph: A handbook for electricians and operators. By Franklin Leonard Pope, 1868

[2] MODERN DICTIONARY OF ELECTRONICS - 3rd Ed. - by Rudolf F. Graf - 1962-1970

[3] Jim Colvin, "ESD failure analysis methodology", Microelectronics Reliability, Volume 38, Issue 11, November 1998, pp. 1705–1714

[4] D.C. Wunsch and R.R. Bell, "Determination of Threshold Failure Levels of Semiconductor Diodes and Transistors due to Pulse Voltages", IEEE Trans. Nuc. Sci., NS-15, pp. 244-259, 1968.

[5] Smith & Shumka et al "A Laser Scanner for Solar Cell Evaluation and Failure Analysis", Advanced Techniques in Failure Analysis-1978

[6] Rutherford, D.H, Perkins, J.F, "Effects of Electrical Overstress on Digital Bipolar Microcircuits and Analysis Techniques for Failure Site Location", EOS/ESD Symposium 1979, pp. 64

[7] T. W. Lee, "Transient damage in Power Transistors" ISTFA, 1979, pp. 130

[8] T. W. Lee, "The Interpretation of EOS Damage in Power Transistors" ISTFA, 1983, pp. 157

[9] M.J. Middendorf et al, "Observed Physical Effects and FA of EOS/ESD Damage on MOS devices ", ISTFA, 1984, pp. 205

[10] J.T. May, "The interpretation of EOS Damage in Power Circuits", ISTFA, 1985, pp. 92

[11] T.W. Lee et al, "Simulation and Characterization of EOS and ESD Damage in MOSFET Transistors and ICs by Capacitive Discharge" ISTFA, 1988, pp. 95

[12] Z.C. Richardson Jr, "Failure Simulations allow Estimation of Overvoltage Condition in TTL Electronics", ISTFA, 1989, pp. 209

[13] D.S. Kiefer et al, "ESD/EOS damage of HCMOS Gate Arrays", ISTFA, 1989, pp. 201

[14] K.S. Willis, "Photoemission Testing for EOS/ESD Failures in VLSO Devices: Advantages and Limitations", ISTFA, 1989, pp. 183

[15] Y. Kitamura et al, "Breakdown of Thin Gate Oxide by Application of Nanosecond Pulses", ISTFA, 1989, pp. 193

[16] R.A. Launer et al, "Interpretation of EOS Damage in NiCr Resistors", ISTFA, 1990, pp. 279

[17] J.T. May, "Interpretation of EOS-induced discoloration ICs", ISTFA, 1990, pp. 143

[18] D. Wilson et al, "Interpretation of Severe EOS damage on Logic Circuitry", ISTFA, 1991, pp. 289

[19] R. Schani et al, "A new IC Failure Mechanism due to Process-Induced Metal Stress Relief", ISTFA, 1992, pp. 413

[20] J.Y. Glacet, "Identification of EOS Failures in semiconductor devices using acoustic microscopy" ISTFA, 1993, pp. 161

[21] L.G. Henry et al, "Lab simulation and signature analysis of a CMOS programmable Logic Product", ISTFA, 1994, pp. 117

[22] L.G. Henry, Mazur, "Basic Physics in Color-Coded EOS Failures", ISTFA, 1998, pp. 143

[23] B. Lisenker et al, "Model of EOS Caused Electrical Failure Screening in CMOS VLSI", ISTFA, 1995, pp. 121

[24] W. Wu et al, "EOS Failures in Power Insulated Gate Bipolar Transistor Modules", ISTFA, 1995, pp. 159

[25] R. Milburn, K.H. Parekh, "Effectiveness of Emission Microscopy in the FA of CMOS ASIC Devices", ISTFA, 1997, pp. 299

[26] J.E. Vinson, “Al interconnect response to EOS”, ISTFA, 1998, pp. 103
[27] Fan Wang et al, “IC failure by EOS”, ISTFA, 2001, pp. 259
[28] J. Vinson, “The Search for the elusive EOS”, ISTFA, 2001, pp. 265
[29] V. Korchnoy, “ESD Correlation between electrical signature and Failure modes”, ISTFA, 2003, pp. 272

For Further Historical Reading

The following documents, while not explicitly referenced, have been included by the authors of this chapter as historically significant, relevant and instructive milestones in the evolution and advancement of the definition, characterization and analysis of electrical overstress.

Most Recent

[30] K.T. Kaschani, Texas Instruments; “What is Electrical Overstress? - Analysis and Conclusions”; Microelectronics Reliability Volume 55, Issue 6, May 2015, pp. 853–862
[31] Alain Kamdem, Normandie Universite, Presto Engineering; Patrick Martin, Fanny Berthet, Bernadette Domengès, Dominique Lesenechal, Normandie Universite; Jean-Luc Lefebvre, Presto Engineering; Pierre Guillot, NXP Semiconductors, “Electrical Overstress Robustness and Test Method for ICs”, EOS/ESD Symposium, 2014
[32] Alan Righter, Ed Wolfe, Jean-Jacques Hajjar, Analog Devices, “Non-EOS Root Causes of EOS-Like Damage”, EOS/ESD Symposium, 2014
[33] T. Smedes, S. Zhao, NXP Semiconductors; Y. Christoforou, YC Industrial Projects (Formerly with NXP Semiconductors), “Characterization Methods to Replicate EOS Fails”, EOS/ESD Symposium, 2014
[34] Richard Wong, Shi-Jie Wen, Rita Fung, Paul Le, Cisco Systems Inc., “System Level EOS Case Studies not due to Excessive Voltages”, EOS/ESD Symposium, 2013
[35] KP Yan, Reinhold Gaertner, CY Wong, Infineon Technologies, “Poor Grounding – Major Contributor to EOS”, EOS/ESD Symposium, 2012
[36] K.T. Kaschani, Texas Instruments; R. Gaertner, Infineon Technologies AG, “The Impact of Electrical Overstress on the Design, Handling, and Application of Integrated Circuits”, EOS/ESD Symposium, 2011
[37] Al Wallash, Hitachi Global Storage Technologies; Vladimir Kraz, BestESD Technical Services, “Measurement, Simulation and Reduction of EOS Damage by Electrical Fast Transients on AC Power”, EOS/ESD Symposium, 2010

2000's

[38] Vladimir Kraz, 3M Company, “Origins of EOS in Manufacturing Environment and It's Classification”, EOS/ESD Symposium, 2009
[39] A. Wallash, H. Zhu, R. Torres, T. Hughbanks, Hitachi GST; V. Kraz, Credence Technologies, “A New Electrical Overstress (EOS) Test for Magnetic Recording Heads”, EOS/ESD Symposium, 2006
[40] I. E. T. Iben, IBM, “The Thermodynamics of Physical and Magnetic Changes to AMR Sensors from EOS at Variable Pulse Widths”, EOS/ESD Symposium, 2005
[41] W. Farwell, K. Hein, D. Ching, Raytheon Corporation, “EOS from Soldering Irons Connected to Faulty 120VAC Receptacles”, EOS/ESD Symposium, 2005
[42] C H Tung, etal., “Physical FA to Distinguish EOS & ESD Failures”, IPFA 2002, pp. 65-69
[43] M D Ker, JJ Peng & H C Jiang, “FA of ESD Damage in High Voltage Driver IC”, IPFA2002, pp. 84
[44] S Voldman, “ESD & FA Models, Methodology and Mechanisms”, IPFA 2002, pp. 57-64
[45] J C Reiner, etal., “Impact of ESD Induced Soft Drain Junction Damage”, IPFA2001, pp. 77-78
[46] Y. Jaimsomporn, S. Phunyapinuant, W. Tan, “Advanced Micro Devices, DC Transient Monitoring and Analysis to Prevent EOS in Burn-in Systems”, EOS/ESD Symposium, 2001
[47] E. Granstrom, R. Cermak, P. Tesarek, N. Tabat, “Seagate Recording Head Operations, Floating Gate EEPROM as EOS Indicators During Wafer-Level GMR Processing”, EOS/ESD Symposium, 2000

1990's

[48] P S Lim & W K Chim, "Latent Damage Investigation on Lateral Non-Uniform Charge Generation and Stress-Induced Leakage Current in Silicon Dioxides Subjected to Low Level ESD Impulse Stressing", IPFA 1999, pp. 156-161

[49] Banerjee, et al., "High Current Effects in Silicide Films for Sub-025um VLSI Technologies", IRPS, 1998

[50] G. Baumgartner, J. Smith, Lockheed Martin, "EOS Analysis of Soldering Iron Tip Voltage", EOS/ESD Symposium, 1998

[51] Vinson & Liou, "ESD in Semiconductor Devices: An Overview, Proceedings of the IEEE", 1998, pp. 399-418

[52] Vinson, "Aluminum Interconnect Response to Electrical Overstress", ISTFA, 1998

[53] Voldman, et al., "High Current Transmission Line Pulse Characterization of Aluminum and Copper Interconnects for Advanced CMOS Semiconductor Technologies", IRPS, 1998.

[54] G L Teh & W K Chim, "Pre-Breakdown Charge Trapping in ESD Stressed Thin MOS Gate Oxide", IPFA 1997, pp. 156-161

[55] McAteer, "Pulse Evaluation of Integrated circuit Metallization as an Alternative to SEM", IRPS, 1997, pp. 217-224.

[56] T N Tang, C Francis & S T Teh, "ESD Failure Fingerprint in Devices", IPFA 1997, pp. 115-120

[57] T S Yeah, "ESD Effects in Power Supply Clamps", IPFA 1997, pp. 121-124

[58] W Tan, K K Goh & D Corum, "EOS Induced Transistor Shift in Submicron DRAMs", IPFA 1997, pp. 196-201

[59] Banerjee, et al., "Characterization of VLSI Circuit Interconnect Heating and Failure under ESD Conditions", IRPS, 1996, pp. 237-245

[60] K. Banerjee, et al., "Thermal Analysis of the Fusion Limits of Metal Interconnect Under Short Duration Current", International Reliability Workshop Final Report Proceedings, Oct. 1996, pp. 98-102

[61] Ramaswamy, S., Li, E., Rosenbaum, E., Kang, S., University of Illinois at Urbana-Champaign, "Circuit-Level Simulation of CDM-ESD and EOS in Submicron MOS Devices", EOS/ESD Symposium, 1996

[62] Yamaoto and Tsuru, "Time-Dependent Temperature Calculations of Aluminum Lines Applied with Electrical Overstress Pulses", Japan Journal of Applied Physics, July 1996, Vol. 35, Part 1, No. 7, pp. 3852-3857

[63] M Beh, etal., "Analysis of HBM & MM ESD Failures in NMOS Devices", IPFA 1995, pp. 111-115

[64] Song, M., Eng, D., MacWilliams, K., "The Aerospace Corporation, Quantifying ESD/EOS Latent Damage and Integrated Circuit Leakage Currents", EOS/ESD Symposium, 1995

[65] Vinson, "NiCr Fuse Reliability A New Approach", Southcon Technical Conference, 1994, pp. 250-255

[66] J. E. Murguia and J. B. Bernstein, "Short-Time failure of Metal Interconnect caused by current pulses", IEEE Electron Device Letters, 1993, Vol. 14, No. 20, pp. 481-483

[67] Wagner, et al., "Extent and cost of EOS/ESD Damage in an IC Manufacturing Process", EOS/ESD Symposium, 1993

[68] Crandel & Bajor, "Non-adiabatic Model for Prediction of ESD Failure of NiCr Resistors", Proceedings of Florida microelectronics Conference, 1992, pp. 71-74

[69] Diaz, C., Kang, S., University of Illinois and Duvvury, C., Wagner, L., Texas Instruments, Inc., "Electrical Overstress (EOS) Power Profiles: A Guideline to Qualify EOS Hardness of Semiconductor Devices", EOS/ESD Symposium, 1992

[70] Maloney, "Integrated Circuit Metal in the Charged Device Model: Bootstrap heating, Melt Damage, Scaling Laws", Proc. EOS/ESD Sym., 1992, Vol. EOS-14, pp. 129-134.

[71] Feeney, M.D., TAOS International, "Mechanically Relay Induced EOS From Wire Bonding Machines", EOS/ESD Symposium, 1991

[72] K C Aw & K C Nech, "CMOS Device performance Degradation Induced by ESD", IPFA 1991, pp. 184-186

[73] V.M. Dwyer, A.J. Franklin and D.S. Campbell, "Thermal Failure in Semiconductor Devices, Solid-State Electronics", Vol. 33, No. 5, pp. 553-560, 1990

1980's

[74] A Urbeieta & S Letorun, "Influence of Microcircuit Integration on ESD Performance", IPFA 1989, pp. 76-79

[75] King, et al., "Electrical Overstress of Non-encapsulated Aluminum Bond Wires", IRPS, 1989

[76] R Y Liang, "ESD/EOS A real Case Study", IPFA 1987, pp. 123-129

[77] Siemsen, K.B., Motorola, Inc., "EOS Test Limits for Manufacturing Equipment", EOS/ESD Symposium, 1987

[78] X Gui & G B Gao, "A study of EOS effect in Thin Metallization", IPFA 1987, pp. 130-135

[79] Bridgwood, M.A., Clemson University, "Breakdown Mechanisms in MOS Capacitors Following Electrical Overstress", EOS/ESD Symposium, 1986
[80] Stephens, C.E., Amos, C.T., British Telecom, "A Study of EOS in Microcircuits Using the Infra-Red Microscope", EOS/ESD Symposium, 1986
[81] Forster, G., RCA Laboratories Ltd., "Protection of Components Against Electrical Overstress (EOS) and Transients in Monitors", EOS/ESD Symposium, 1984
[82] Ito, et al., "The Physics and Reliability of Fusing Polysilicon", IRPS, 1984, pp. 17-29
[83] Pierce, D.G., Perillat, Jr., J., Shiley, W.L., Booz, Allen & Hamilton, Inc., "An Evaluation of EOS Failure Models", EOS/ESD Symposium, 1984
[84] Ash, "Semiconductor junction non-linear failure power threshold: Wunsch-Bell revisited", EOS/ESD Symposium 1983, pp. 122-127
[85] Enlow, E.W., Buden, B.N., Gieri, V.A., Young, P.A., BDM Corporation, "Power Failure Modeling of Integrated Circuits", EOS/ESD Symposium, 1983
[86] Noel, P.H., Dreibelbis, D.H., IBM Corporation, "EOS or ESD: Can Failure Analysis Tell the Difference?", EOS/ESD Symposium, 1983
[87] D. G. Pierce, "Modeling Metallization Burnout of Integrated Circuits", ESD Sym. Vol. EOS4, 1982, pp. 56-61
[88] Greve, "Programming Mechanism of Polysilicon Resistor Fuses", IEEE Trans. On ED, ED-29, N. 4, April 1982, pp. 719-724
[89] Volmerange, H., TRW, "An Improved EOS Conduction Model of Semiconductor Devices", EOS/ESD Symposium, 1982
[90] Hays, R.A., USAF, "Weapons Laboratory, EOS Threshold Determination of Electro-Explosive Devices", EOS/ESD Symposium, 1981
[91] Kusnezov, N., Smith, J.S., Lockheed Palo Alto Research Laboratories, "Modeling of EOS in Silicon Devices", EOS/ESD Symposium, 1981
[92] Pierce, D.G., Durgin, D.L., Booz, Allen & Hamilton, Inc., "An Overview of Electrical Overstress Effects on Semiconductor Devices", EOS/ESD Symposium, 1981
[93] Volmerange, H., TRWYoung, P.A., Karaskiewicz, R.J., BDM Corporation, Alexander, D.R., Sandia National Laboratories, "Electrical Overstress Investigations in Modern Integrated Circuit Technologies", EOS/ESD Symposium, 1981
[94] Wunsch, D.C., BDM Corporation, "An Overview of EOS Effects on Passive Components", EOS/ESD Symposium, 1981
[95] Domingos, "Basic Considerations in Electro-Thermal Overstress in Electronic Components", ESD Symposium 1980
[96] Durgin, D.L., Booz, Allen & Hamilton, Inc., "An Overview of the Sources and Effects of Electrical Overstress", EOS/ESD Symposium, 1980

1970's and Earlier

[97] Kusnezov, N., Smith, J.S., Lockheed Palo Alto Research Laboratories Rutherford, D.H., Raytheon Company, Perkins, J.F., Hi-Rel Laboratories, Inc., "Effects of Electrical Overstress on Digital Bipolar Microcircuits and Analysis Techniques for Failure Site Location", EOS/ESD Symposium, 1979
[98] Kusnezov, N., Smith, J.S., Lockheed Palo Alto Research Laboratories, "Modeling of Electrical Overstress in Silicon Devices", EOS/ESD Symposium, 1979
[99] Davidson, et al., "Fusing Mechanism of Nichrome Thin Films", IRPS, 1976, pp. 173-181.
[100] Kenney, "Fusing Mechanism of NiCr Linked Programmable read-Only Memory Devices", IRPS, 1976, pp. 164-172.
[101] Kinsbron, et al., "Failure of small Thin-Film Conductors Due to High Current-Density Pulses", IEEE Trans on ED, ED-26, No. 1, Jan 1979, pp. 22-26.
[102] Madison, J.A., Westinghouse Electric Corporation, "The Analysis and Elimination of EOS Induced Secondary Failure Mechanisms", EOS/ESD Symposium, 1979
[103] Smith, "Analysis of Electrical Overstress Failures", IRPS, 1973
[104] D. M. Tasca, "Pulse Power modes in Semiconductors", IEEE Trans on Nuc. Sci. NS-17, 1970, pp. 364-372.

Chapter 2: EOS Damage in the Factory and Field

Alan Righter, Analog Devices
Charvaka Duvvury, Texas Instruments (Retired)
Jim Miller, Freescale Semiconductor

2.0 Outline

This chapter will first summarize the motivation for the EOS field returns analysis, conditions that could cause EOS damage in the factory and the field, how a determination of EOS can be made, and how these failures exhibiting EOS damage from EOS or other non-ESD root causes can be distinguished from EOS damage resulting from ESD events. Section 2.2 on transients discusses ways by which transients can couple into a system causing EOS damage. In Section 2.3, the development and description of the industry EOS survey is given. Section 2.4 describes the results, both in graphical form and summary, of the different questions followed by notable comments from companies on their experiences with EOS damage both within their company and with their customers. This will lead to a summary of the impact of EOS damage, both in terms of time and economics, to the electronics industry. The full EOS Survey that was sent out appears in Appendix A.

2.1 Motivation for Field Returns Analysis of Failures Exhibiting EOS Damage

EOS is consistently one of the "high bars" on product failure Pareto charts in the electronics industry. EOS occurrences can be expensive to the entire supply chain (OEM, system supplier, module supplier, and IC supplier) in terms of time to resolve and opportunity cost. In most high reliability applications, if the failing devices in the board or product can be accessed, the devices are returned to the supplier and supplier resources are used to diagnose the failure and determine root causes of failure. Depending on the number of systems or devices returned the potential exists to affect long term reliability of an entire program unless the root cause(s) of the failure mechanism is found and an effective fix / solution is found and implemented. Delays in end product cycle time and mass production of systems often results.

As IC technologies scale and voltages decrease, and systems become more complex, the amount of energy transfer into systems necessary to produce EOS has been decreasing, and the damage can involve a larger area of the device.

2.1.1 Examples of Damage Resulting From Different Root Cause Mechanisms

Various root causes of EOS damage give rise to many different damage characteristics in ICs. Chapters 4, 5 and 6 present more information on this through various literature and case studies. Signatures associated with mishandling, signal / supply overshoots or misapplication often can involve package and IC material damage, and are more extensive in a product than failure signatures resulting from events in the measurable ESD regimes. High power transients from these root cause events can involve damage including metal burnout and significant electromigration (often in several locations), heating to the point of carbonized material on the surface of die, blown open bond wires, package melting, delamination, reflowed metal supply or ground buses, and blown holes in silicon / contact or substrate regions. Often the EOS damage signatures can be seen

optically. There can be several regions of damage, involving several different failure mechanisms. Field induced events, charged person discharges or charged devices resulting in a discharge into or through a component (as a result of unpowered handling) often result in more localized damage areas involving less area and specific material changes (pinholes in one or more transistor gate oxides of a device, or junction damage in one or more devices in a current path).

2.1.2 What Information is Expected from these "Returns Exhibiting EOS Damage?"

Root cause diagnosis of EOS damage requires knowledge of the application at the time of the damage. This involves the following:

- where in the application or system the damage occurred
- environmental conditions at the time of the damage or during the test which revealed the damage, in terms of automotive, this would include the environment within the particular location of the car
- schematic / layout of board devices in the application
- details of the supply, ground and input/output (IO) connections and voltages at the time of damage
- details on the interconnection of devices on the board which could provide paths for the electrical stress
- any possible “precursors” to damage (on the supplier side, determination of IC process, IC assembly yield, test issues, or results of device analysis indicating a weakness; on the system manufacturer side, tester programming / hardware, or connection related issues in the application)

2.1.3 What is the Realistic Percentage of Devices that Customers do Return?

Many customers using products in non-high reliability applications would only provide a single return exhibiting EOS damage as a representative example and they may not report a rate of damage. The undisclosed devices would then be a hidden cost (customer would just buy a new one, or supplier would just supply a new device). However, customers supplying high reliability systems (such as automotive, non-space aerospace, pacemaker manufacturers, medical products) return every damaged device and expect failure analysis with results and root cause determination from an investigation on every single device, involving teams of design / product / FA from customer and supplier. So overall there is no “consistent” percentage across the electronics industry.

2.2 Transients

There are many ways a transient can enter into a system. Some may be from a directly applied source including, but not limited to:

- overvoltage spikes on supplies
- charging / discharging of large value capacitors directly into system pins
- long charged cables connecting directly into system pins
- a system being supplied with power before its connection to ground (connection of a board into a system plug contacts supply pins before ground pins)

Other more indirect ways could involve:

- Process induced – Such as those in assembly or IC misprocessing resulting in low breakdown, direct shorting, or unintended high current density path from device die to IC pin.
- Charged board – Sudden discharging of a charged board to a ground potential can result in discharge paths through the board's supply and ground tracks which directly route to or through components causing excessive current densities and component damage.
- Test induced – Excessive voltage transients resulting from incorrect power supply switching or incompatible switch control voltages, glitches on supplies, program induced misbiasing of supplies, incoming testing using charged multimeters.
- Coupling of external radiated energy into unprotected devices of a system – This can occur in those applications which generate or are in the range of this type of energy and which can also cause high voltages / currents that cause damage in systems and components.

Components and systems which have been compromised by insufficient ESD control may be prone to EOS damage upon application of a direct or indirect energy transfer as above.

These stimuli can immediately (or later during operation) produce damage signatures typical of EOS damage to components, including large area damage to the IC die, metal burnout, carbonized molding compound (for packaged components), wirebond thermal fusing / opens, etc. The thermal energy can spread to induce damage on the board itself and to other components of a board or system.

2.3 EOS Survey for Gathering Data on EOS Damage

2.3.1 Survey Form and Description - How was the Survey Conducted?

The Industry Council created an EOS survey for the purpose of collecting data from a broad set of people within the electronics industry. A list of electronics industry companies and associations, as well as institutions and conferences, etc. was identified and an email was sent to contacts (at their company address) within these associations. The contacts were invited to submit the EOS survey themselves for the company or forward the survey to the correct point of contact in their company for submittal. The survey was placed on the Industry Council web site so that people could request online to participate. To reach critical Asian companies, the survey was also translated into Chinese, Japanese and Korean. To access the survey, respondents gave their email address (similar to what AEC does), then they were allowed to download the survey (a PDF file allowing user entry). To ensure simple and anonymous feedback, no company specific or email address information was part of the collected survey data. The survey results (the returned pdf files) were extracted automatically and formatted into a .csv report file. For the checkbox or single item entries, charts with question titles were derived showing pictorial results which are summarized in the results section below. Additionally, questions requiring comments as answers were asked and the anonymous comments were collected. The EOS Survey is included in Appendix A.

Note: At the time the survey was done, many references to EOS were made in terms of "EOS failure". The figures in Section 2.3.2 and subsequent comments, as well as the Survey itself in Appendix A, keeps these references. But it must be clarified that the failed devices should not be referred to as "EOS failures" but rather "failures exhibiting EOS damage". Root causes of EOS can

come from many sources, and devices and systems are not designed to be immune to EOS. This distinction is maintained throughout the rest of WP4. It is expanded in Chapter 4 and in the case studies of Chapter 5.

2.3.2 EOS Survey Results

The remainder of this chapter discusses results of the EOS survey. Results from single selection questions will be presented in graphical form followed by discussion of the results. The end of this section will feature notable written response answers to questions asking for comment response.

2.3.2.1 Demographics of Companies Reporting EOS Data

Eighty-one responses to the EOS survey were received from Oct. 2012 to May 2013. Three questions were asked regarding company demographics. Figure 3 shows the market segments in which each company operates. Note that respondents were allowed to select multiple segments, if applicable.

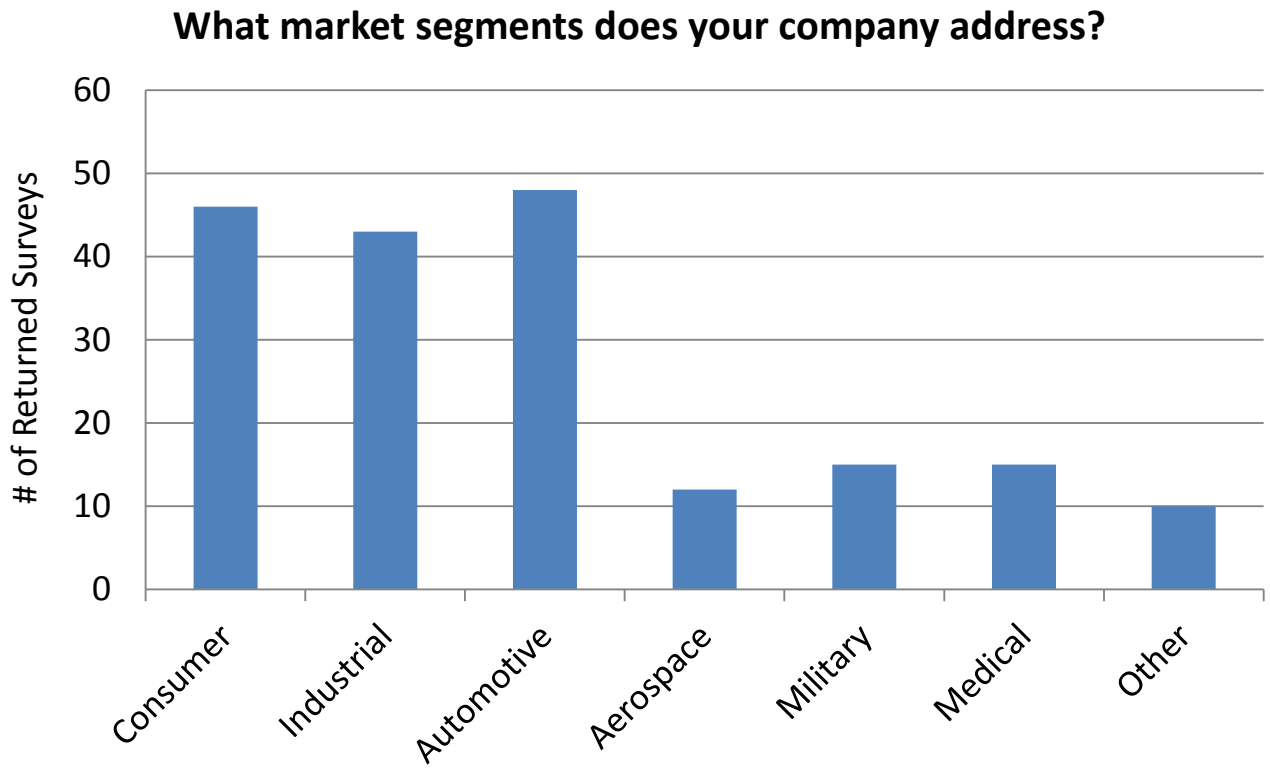


Figure 3: EOS Survey Question 1a

The majority of respondents serve the consumer, industrial and automotive markets with each returning over 40 responses. The aerospace, military and medical markets were also well represented, but with about a third as many responses as the prior groups.

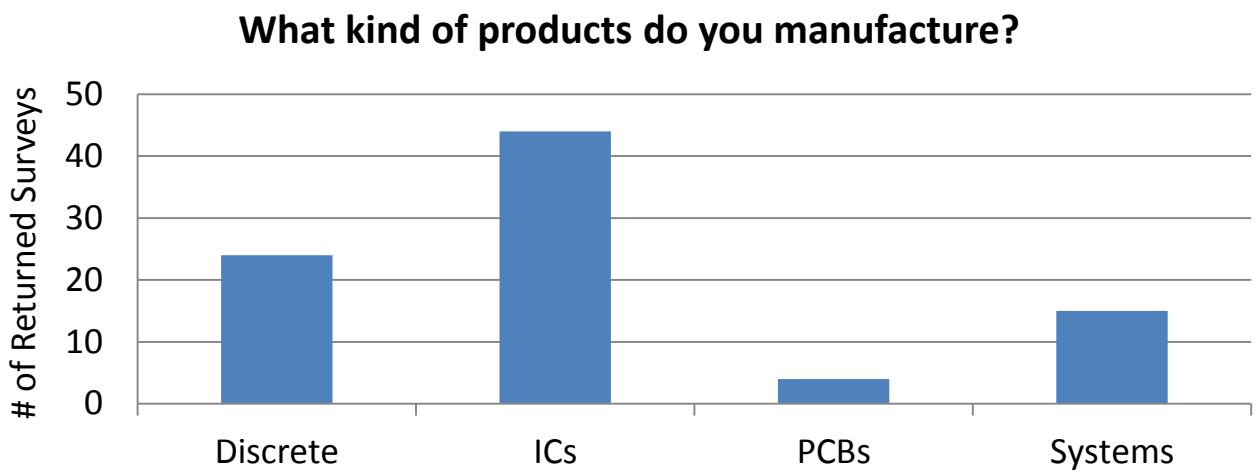


Figure 4: EOS Survey Question 1b

Figure 4 illustrates that most of the respondents work for companies which sell discrete components or integrated circuits. Printed circuit board manufacturers were least represented, with only 4 responses. However 15 final system manufacturers (OEMs) participated in the survey.

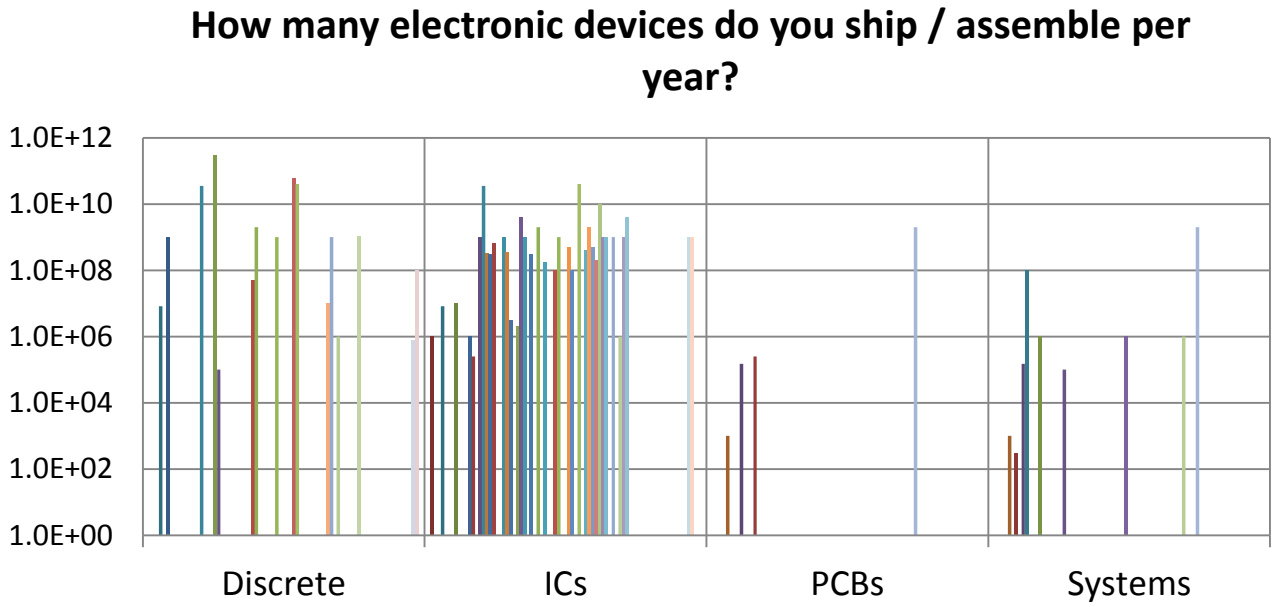


Figure 5: EOS Survey Question 1c

The final demographics related question referred to the number of electronic devices each company assembled and shipped per year. You can see in Figure 5 that the "number of units shipped" responses varied from a few hundred to several billion across the discrete, IC, PCB and system space. Clearly the majority of the companies ship large volumes of product.

2.3.2.2 Industry Data on EOS Classification

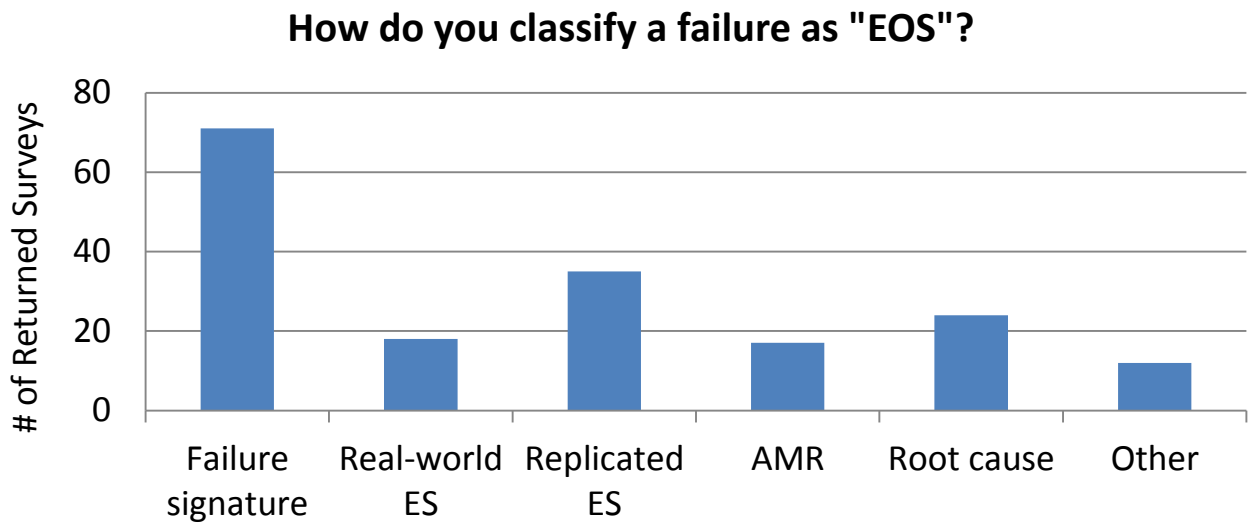


Figure 6: EOS Survey Question 2a

Figure 6 shows 71 of 81 respondents classify EOS based on a failure signature (exhibiting EOS damage), indicating obvious severe damage as a key criteria of failure. Additionally, 35 of 81 respondents determine if they can replicate the damage with an electrical stress as a criteria for classifying as EOS (note: ES in the above graph is electrical stress).

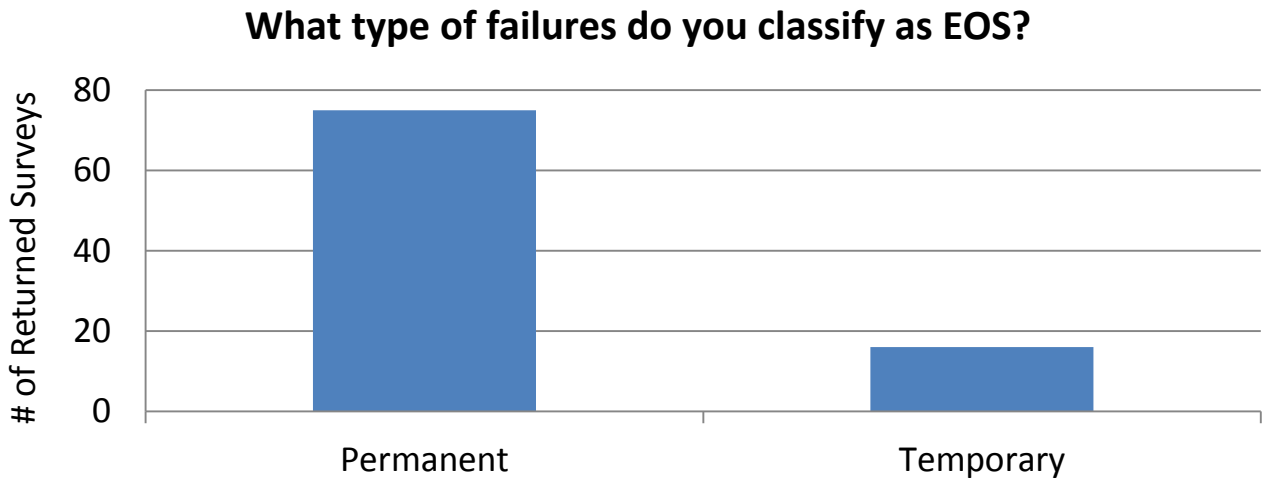


Figure 7: EOS Survey Question 2b

Figure 7 shows 75 of 81 respondents would classify permanent damage as EOS damage. Only 16 of 81 would also classify non-permanent (intermittent or resettable) as an EOS damage mode.

2.3.2.3 Failure Rates, Main Causes, and Origin of Failures

The following graphs show reported EOS failure rates (as percentages of both total and electrical failures), reported causes of failures, and at what stage of the product life the failures occurred.

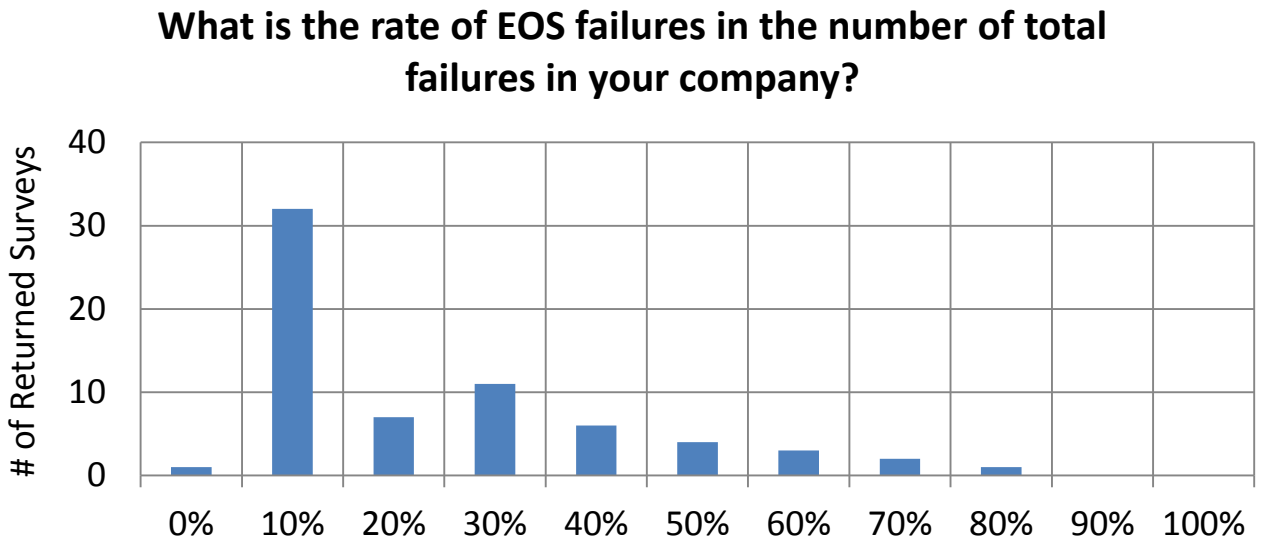


Figure 8: EOS Survey Question 3a

Figure 8 shows nearly every respondent reported a non-zero EOS failure rate (in terms of percentage of total failures). The average percentage of EOS failures out of total failures was about 25%. One respondent reported a zero percent rate; nine reported EOS failures as being equal to or greater than 50% of their total failures.

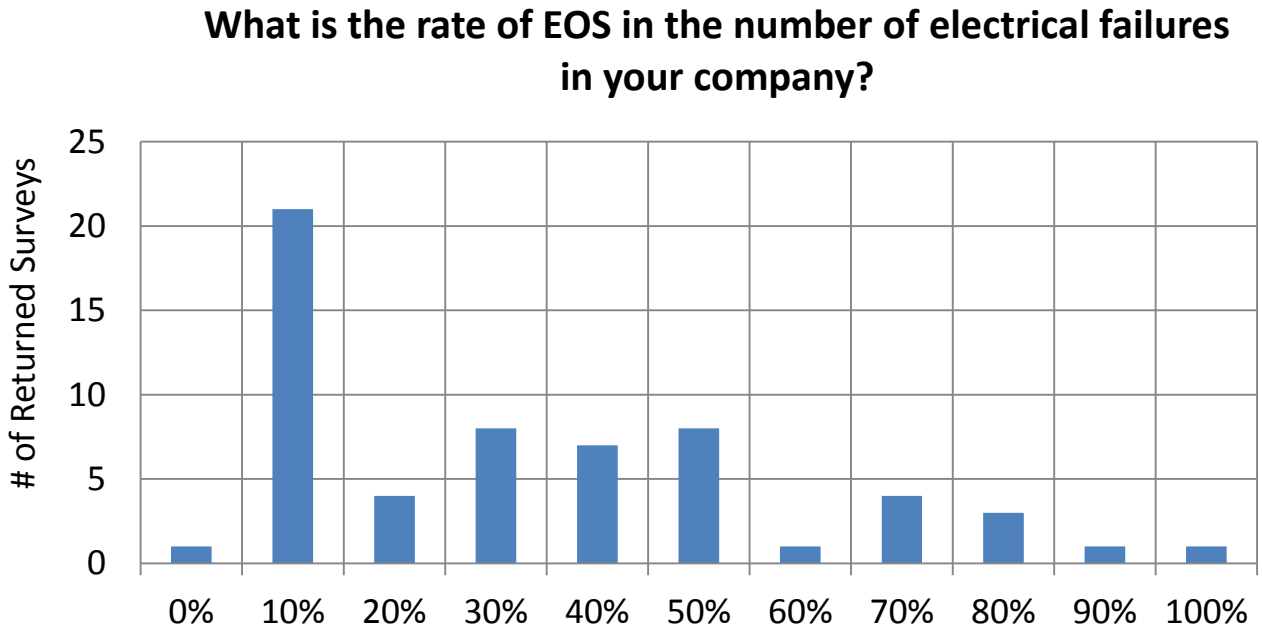


Figure 9: EOS Survey Question 3b

Figure 9 shows nearly all respondents reported a non-zero percentage of EOS returns as related to the total percentage of electrical failures (looking at total electrical failures removes the "no trouble found" category). The average percentage of EOS returns out of total electrical failures was about 30%. Only one respondent reported a zero percent rate; 17 of 81 respondents reported EOS returns as being equal to or greater than 50% of their total electrical failures.

It should be noted that for respondents reporting greater than 20% of total failures being EOS-related or 30% of total electrical failures being EOS-related, this would make EOS the largest bar on the Pareto chart of that responder's known causes of returns.

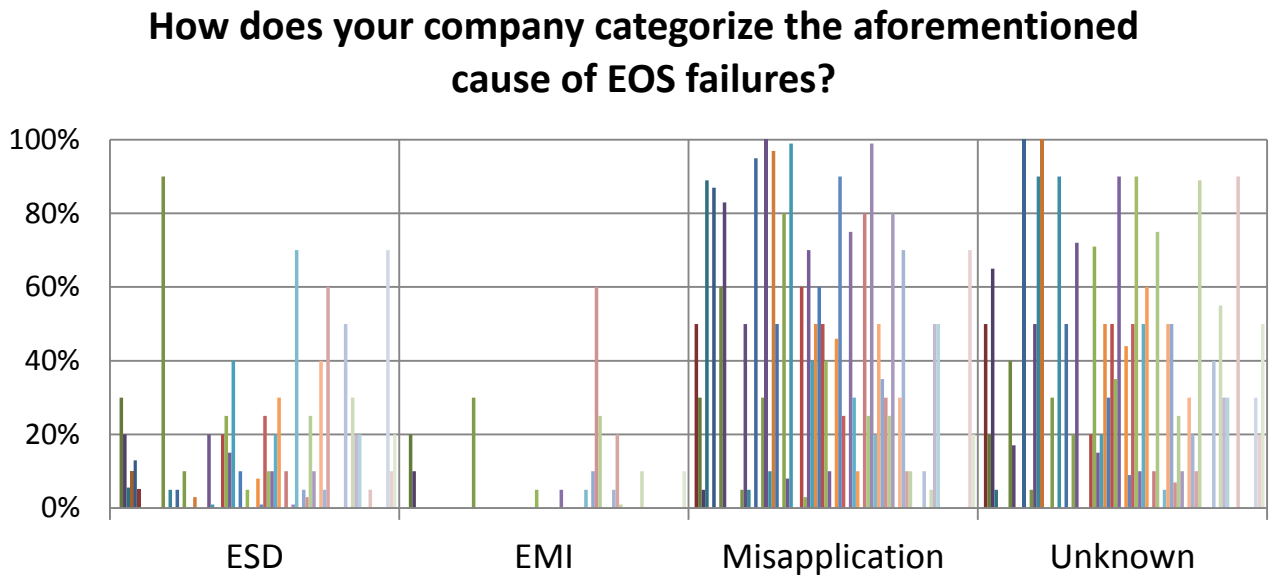


Figure 10: EOS Survey Question 3c

Figure 10 shows a distribution for the four main reported causes of EOS damage as described in the fishbone included in the survey. Within each graph response category, the composite from all 81 companies are shown. In other words, the survey limited the response options to the 4 categories of ESD, EMI, Misapplication, and Unknown. The Y-axis shows the percentage out of 100% for each category with the sum of all 4 categories always equal to 100%. The same colored bar in each category represents one company's response percentage for that category. This visual format shows collectively how widespread each main cause is in the industry.

The most widely reported cause of EOS damage was misapplication. Misapplication failures include hot plugging (plugging into a powered socket; this had the most respondents, 21 of 81), unintended overvoltage on supplies occurring during testing, component misinsertion or misalignment, etc. There was a wide distribution of reported misapplication percentages, from 0 to nearly 100%.

The second highest reported percentage cause was "Unknown", having almost as high a reported occurrence rate as misapplication. These returns could not be, or were not, traced to a root cause. There was a wide distribution of total percentages in the unknown cause category, similar to misapplication.

The third highest reported percentage cause of EOS damage was some form of ESD (charged board or charged cable events, system level events, charged devices discharging, incomplete or nonexistent ESD controls, etc.). Of the companies reporting ESD as a cause, the most common percentage of EOS damage being due to ESD was in the 10-19% range with a close second group of respondents reporting a percentage of 20-29% due to ESD.

The lowest reported percentage cause of EOS damage was EMI (which includes coupling and external non-contact events) which was reported by only 14 of 81 respondents, and the percentage incidence of reported EMI was lower than that of the other three groups, an average of 5%. Only 5 of 81 companies reported 20% or more failures due to EMI, with one respondent reporting a 60% failure rate. It is possible the low percentage reported for EMI is due to the difficulty in getting to a root cause for this category.

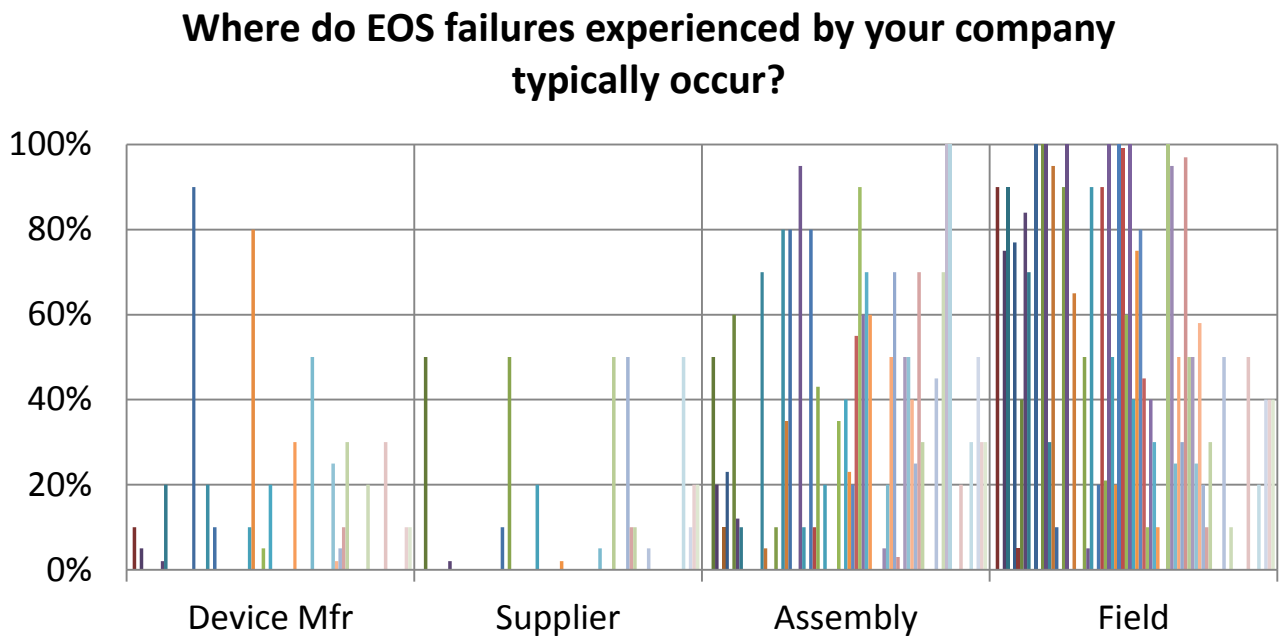


Figure 11: EOS Survey Question 3d

Figure 11 shows the collective company response identifying where failures exhibiting EOS damage occurred in the electronic/system supply chain. Locations were divided into four categories: Device Manufacturer, Supplier, Assembly and Field. It should be noted that some overlap was expected, as respondents in one category could be in a category "earlier in the product cycle" with respondents in a later stage in the product cycle unlikely to classify failures in an earlier category.

The most common reported origin of EOS damage was “Field”, with an average percentage of over 40%. There was a wide distribution in the percentages respondents gave with an origin of “in the field” (Figure 11 Field column).

The second highest reported origin of EOS damage was assembly-related. Most companies reported some percentage related to “Assembly” as an origin of EOS damage. Indicating “Assembly” as an origin of damage was somewhat lower than “Field” at an average of 30%. This category showed a

wide distribution, ranging from less than 5 % to 100 %, with 13 of 81 companies reporting 60% or more of their failures occurring in assembly.

From these above two categories, when taking into account the reported location of where the EOS damage occurred, it is observed that misapplication in assembly or field resulting in EOS damage represents by far the largest reported location / root cause combination.

In the second lowest reported percentage category, 22 of 81 reported "Device Manufacturer" as the origin of EOS damage. The average percentage in this category was around 20%. 6 of 81 reported 30% or higher percentages (the greatest was 80%), while most others reported 20% or less.

In the lowest reported category, 14 of 81 respondents reported "Supplier" as the origin of EOS damage. Of these reports, the average percentage in this category was under 20% with greater than half reporting 10% and 5 of 81 reporting 50%. It should be noted that "Supplier" could have a different meaning depending on the reporting company's position in the manufacturing chain. For example, a device manufacturer's "Supplier" may be a contractor testing or assembly facility. An OEM's "Supplier" may also be reported as a "Device Manufacturer". This may account for the low reported "Supplier" location percentage.

2.3.2.4 Other Reported Causes of EOS

One outcome of the survey was that a number of respondents indicated EOS causes which did not fit well into the "fishbone" categorization of failures in the EOS survey. These reported causes included:

- oscillation
- linear mode
- shoot through
- vendor quality
- welding (soldering)
- electrostatic coating
- outsourced processes
- fails at card lamination (customer)
- connection to neighboring device
- weakness in PCB design

2.3.2.5 Diagnosis, Importance of EOS Reduction, and Failure Reports

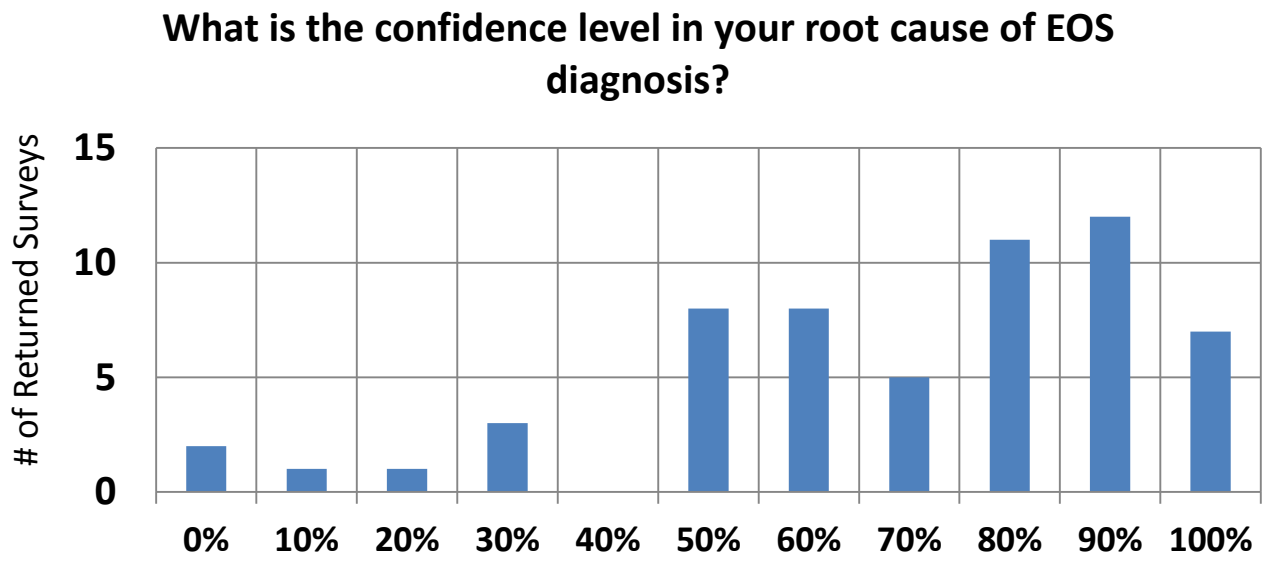


Figure 12: EOS Survey Question 3f

Figure 12 assesses respondent confidence in determining root causes of EOS damage. A majority of respondents were confident that EOS damage could be correctly diagnosed and attributed to a root cause. Of the majority reporting 50% or higher confidence, the average is 80%. In review of responders showing a higher confidence level (70 % – 100 %), a majority of those responders also reported root causes most often which included hot plugging, overshoot / overvoltage / power surge, and misorientation. Table 1 summarizes the top 3 root causes from those companies with a confidence level of 70% or higher. Note not all companies gave details on the top root causes found.

Table 1: Top Root Causes for High Confidence Responders

Confidence in Diagnosing Root Cause (Percent)	Company Identifier	Root cause 1	Root cause 2	Root cause 3
100	6	Hot Plugging	Power Surge	Test Software
100	15	ESD; but very rare		
100	53	Assembly/Handling	Mis-Insertion	Power Supply (sequencing, spike, ...)
100	59	Hot Plugging	Ungrounded Equipment	Wrong polarity
100	61	Wrong parameters at testers (voltage or current is too high)	Hot plugging	
100	80	Burnt Features	Disconnect Bonding Wire	Specific Device Damage
90	12	Single Event Latch up	Transient Latch Up due to internal component noise	Poor documentation from supplier.
90	28	Fails at card lamination (done by customers) - exact root cause/model unknown!	Missing ESD protection equipment at customer assembly	
90	43	Overstress at supply pins	Overstress at the external buses, like I2C	Caused by connected neighboring devices
90	56	Unconsidered or hidden inductivities in circuitry design w/o protection for critical devices	EMI due to long cables between components or neighbored high power circuitry	missing derating combined with/ or "sportive" device specifications
90	62	ESD	EMI	
80	11	Hot plugging	System level design	component (date codes, process changes)
80	32	Overvoltage during Burn In	Overvoltage during Test	Misorientation during Test
80	54	Overvoltage	Hot Plug	
70	8	Breakage in ground path	Overstress of ESD materials	Faulty component
70	23	Instable Tests : Test Equipment Disorder	Misorientation	
70	42	Hot plugging	Inductive switching	Spec violations
70	70	Over current		

For companies reporting a low percentage in finding root cause, root cause "cannot be determined" was a likely outcome. This could be a consequence of not having complete information on conditions, or difficulty with replicating the environment that produced the initial damage. For example, for damage reported to be due to EMI, analysis to root cause may be very difficult. It is a goal of this document (in Chapters 4 and 5) to help give more information on how to trace an EOS diagnosis back to the root cause of the damage including root causes such as EMI.

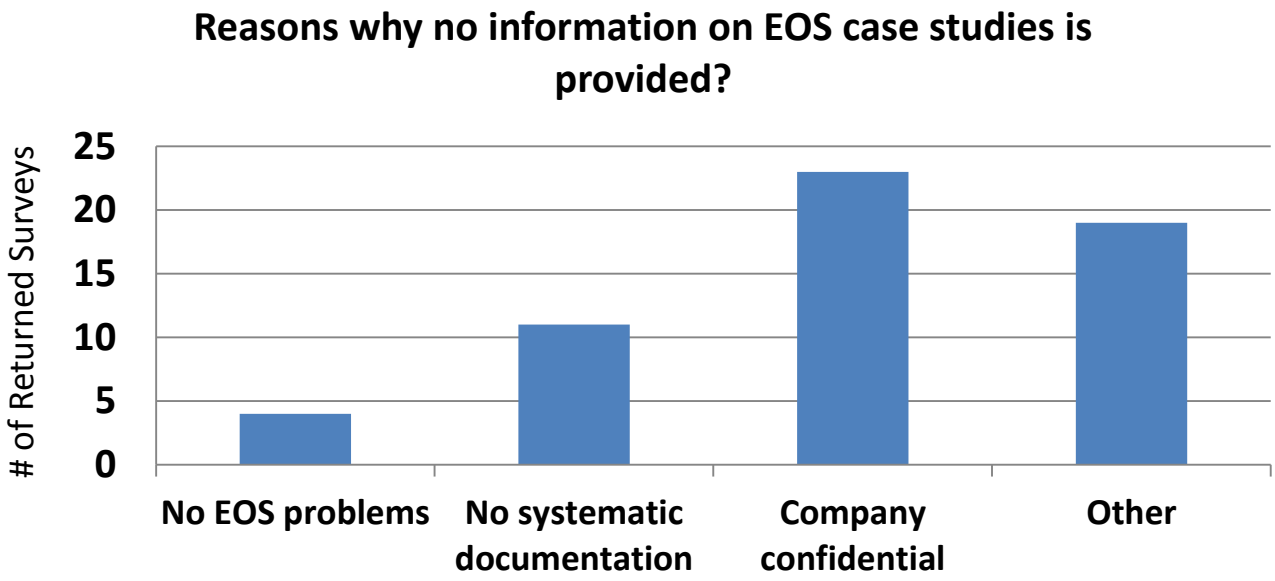


Figure 13: EOS Survey Question 4

Question 4 of the survey asked for reasons why information on case studies of EOS could not be provided in the course of investigation. Figure 13 summarizes the results for companies not providing case studies. Confidentiality was a main reason, cited by 23 companies. A significant number cited "other" and did not elaborate. "No systematic documentation" was cited in 11 cases.

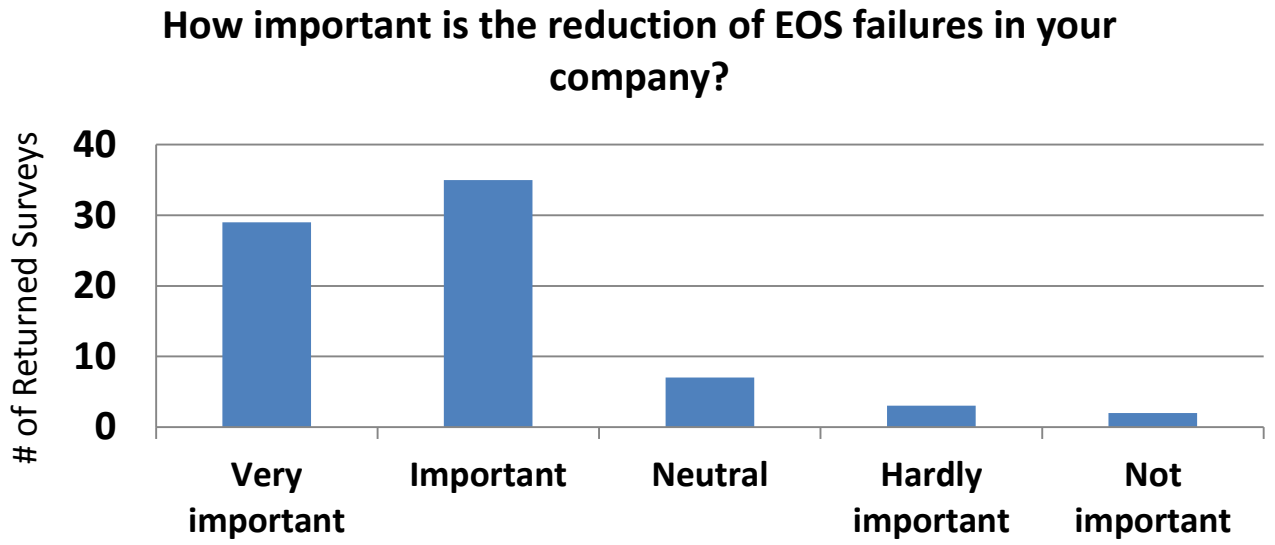


Figure 14: EOS Survey Question 5a

Figure 14 shows the collective company response of perceived importance of reducing their EOS damage failure rate. 85% of respondents indicated a reduction of EOS failures was either "important" or "very important" to their company.

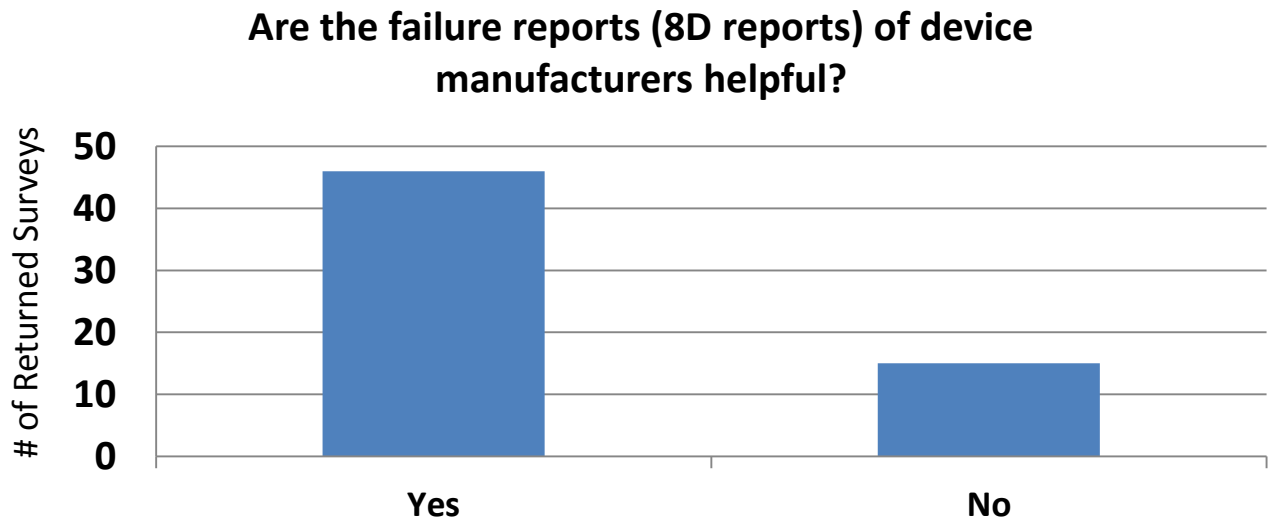


Figure 15: EOS Survey Question 6a

For those respondents familiar with the "8D" ("8 Disciplines of Problem Solving" was first attributed to Ford Motor Company in the 1980s as a new process to address and solve difficult issues) problem solving methodology of system quality issues, Figure 15 shows that 75% of respondents indicated 8D reports are helpful to them. Although this result does not tie directly to reporting of EOS related issues, it indicates the 8D methodology would be helpful for investigating issues from EOS.

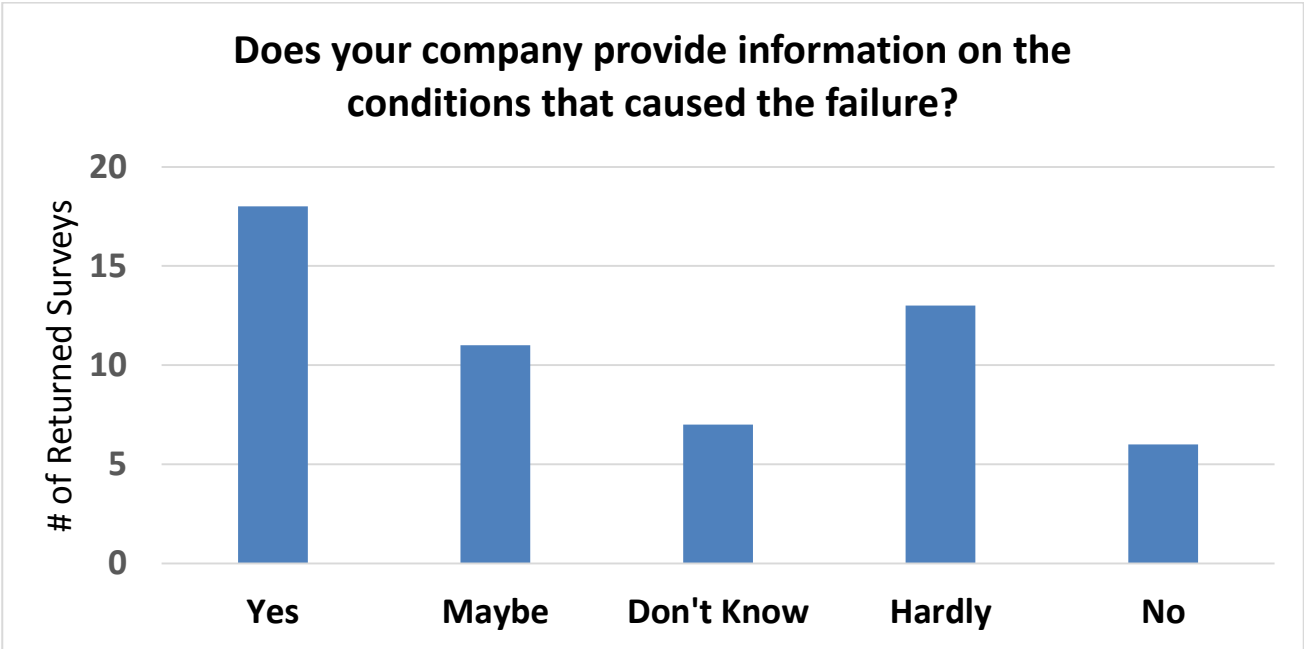


Figure 16: EOS Survey Question 6c

A follow-on question to the 8D report importance question asked if the surveyed company would provide information on conditions that could have caused a failure exhibiting EOS damage.

Although the highest percentage (34%) of companies reported they did report conditions, Figure 16 shows there was a wide distribution indicating many companies provided incomplete or no information on the failure conditions. This is a response indicating the need for improved communication in the EOS damage root cause diagnosis.

2.3.2.6 Responses on EOS Problem Minimization and Rate of Success

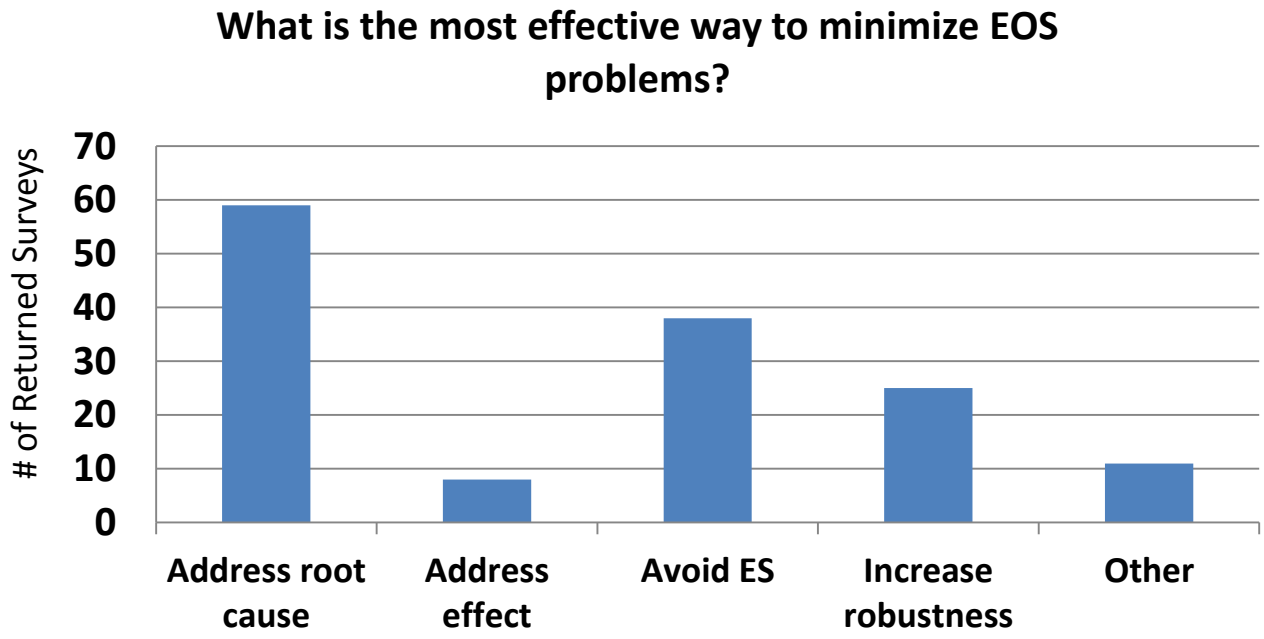


Figure 17: EOS Survey Question 7a

Figure 17 shows the collective response to the question asking what the most effective way is to minimize EOS problems. The wide majority indicated addressing the root cause of the failure was the most effective way. Nearly half the respondents indicated avoiding the particular electrical stress was also a most effective way. Over 25% of the respondents felt that increasing the device robustness overall would help minimize EOS problems.

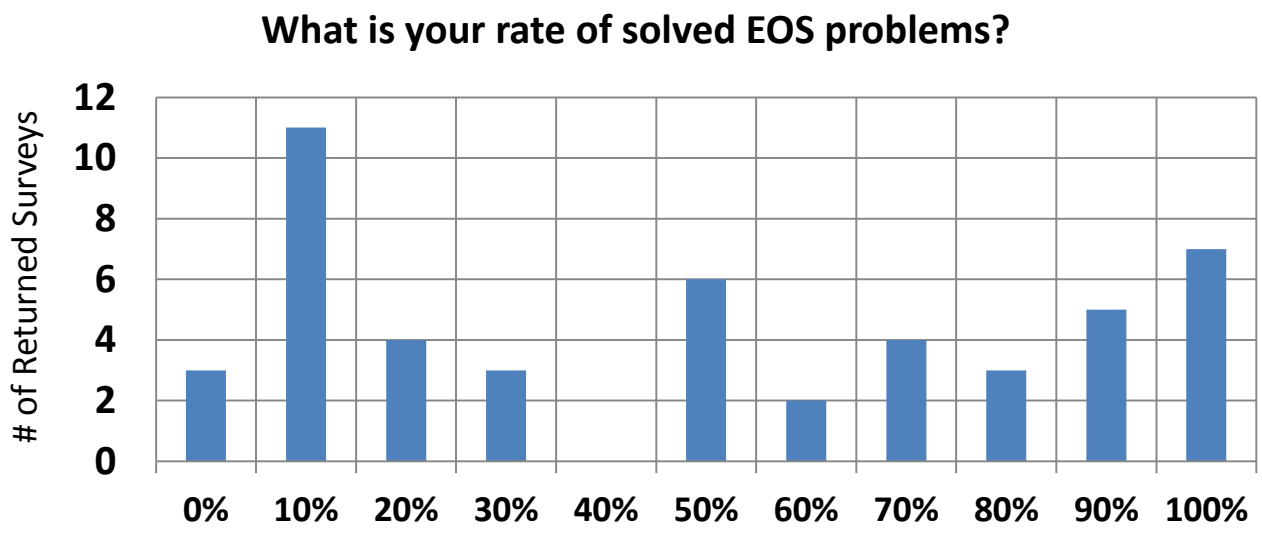


Figure 18: EOS Survey Question 7b

Figure 18 shows the collective company response as to the "rate" of solved EOS problems. A wide distribution is indicated; there are higher percentages of responses selecting "very few", 50%, and 90-100%. Looking over the last three survey questions, it can be seen that the lack of detailed industry wide information on the conditions of damage and addressing root cause creates a wide disparity in actually solving EOS problems. This is an area where communication and working together with more information could result in improvement.

2.3.2.7 AMR Usage and Importance

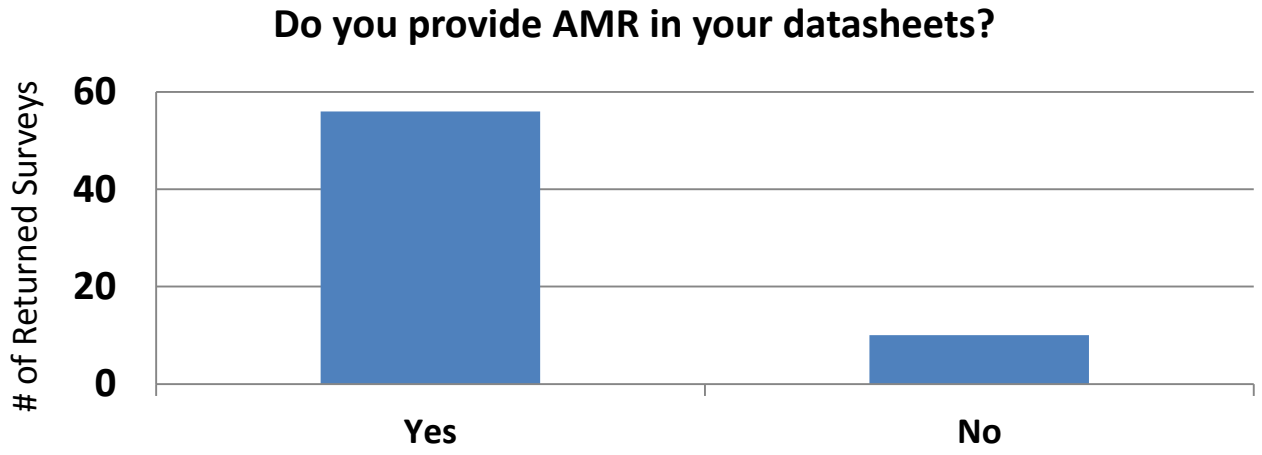


Figure 19: EOS Survey Question 8a

Figure 19 shows the collective response to whether companies provide absolute maximum ratings values in product datasheets. The wide majority do provide AMR values.

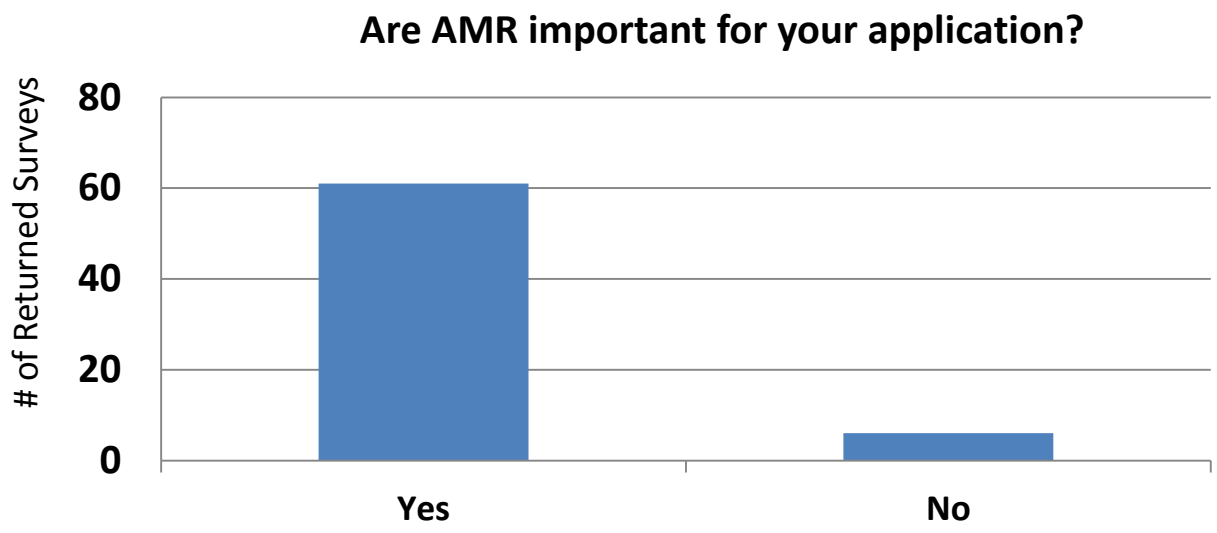


Figure 20: EOS Survey Question 8b

A similar percentage of respondents reported in Figure 20 that they consider AMR important in their application. Nearly all responses were positive indicating suppliers, customers and OEMs agree on the importance of AMR.

2.3.3 Notable Industry Comments on the EOS Survey

In addition to the graphical response data, the EOS survey provided a forum for respondents to give specific comments on EOS issues. These responses included descriptions of how EOS is perceived within their company, how their customers view EOS, whether information on failure conditions is useful, how higher energy EOS damage could be differentiated from damage resulting from ESD events, etc. Below are some of those responses.

- *"We have spent considerable effort educating our customers on the difference between EOS and ESD. We request that the Industry Council take some care not to cause confusion. Very few EOS failures are due to ESD events - although we do have examples where the ESD cell is the weak point that is sensitive to an EOS event."*
- *"As an IC supplier, we often see EOS induced failures, but receive very little to no feedback from the customer if they were able to identify the source of the EOS, or if any additional actions were taken as a result of the failure analysis provided by the IC manufacturer."*
- *"EOS reduction/prevention should be a joint effort including (material supplier), IC suppliers, system applications to be more effective to find out. In my opinion, customers, modules and end-customers are even less aware of maximum applicable electric stress than it was the case in the past."*
- *"If something goes wrong, the attitude is often: the device manufacturer has changed the process, because it has worked in the old module-versions."*
- *"There is no longer a 'sit-down-and-think-about' attitude in case of a problem on system level. This leads to the problem that we do not get any clue from the customer side, what*

could happen. So we have to spend a lot of effort to prove a) it is not the process and b) do customer-side work and replicate a stress that gives us the same failure signature. When we are lucky, we get at least a very honest customer who tells us what he has done and what he has not done. So at least we have the chance to understand what has happened. Unfortunately in many cases a violation of already known text-book ESD/EMC/EOS was the "root" cause."

- *"A reliable way for characterizing AMRs is missing. Actually there are many definition/characterization ways presently used, which makes the definition of AMRs quite fuzzy as to how each manufacturer defines them. A comprehensive way is missing. Standardization could most probably help here.*

  Examples of 'fuzzy' AMRs are:

  (1) A maximum supply voltage can be very close to the breakdown voltage of a given pin. How do we characterize this? How far should it be located? How can we take process spread in account for a given quality performance of the product in the field?
  (2) When characterizing for ESD, how much higher should the FAIL level be in order to specify a given PASS level?
  (3) Why some products have ESD-related AMR and some do not? Some AMRs shouldn't be compulsive for all products to be mentioned in the datasheet?
  (4) How to specify AMRs related to a transient performance of the IC?
  (5) How to test AMRs? Can ATE testing be enough and under which conditions?

  An AMR is a publishable parameter (stated in the datasheet). A priori it should not be dependent on the underlying manufacturing process. How can we guarantee this (such as in the case of process change or use of a new process)? AMRs related to misapplication/EMI types of EOS are missing."

- *"Information is usually missing with respect to the real failure conditions at the system-maker, the car-manufacturer or from the user at the field. All should provide more information regarding the failure context (e.g. operation that was taking place during the failure and if possible voltages / currents available during that operation – for instance oscilloscope pictures). Also, handling tips should be available for products that do not fulfill the basic ESD specifications. The IC manufacturer should also provide hints in the 8Ds on how to mitigate EOS/ESD for a specific failure."*
- *"We worry about EOS (for a product) when there are more than 2 quality hits on a product in a particular quarter (internal or external) with an EOS signature (very high current increase, FA result, field returns from one or more customers)."*

2.3.4 Top 4 Reported EOS Root Causes and Confidence Level

The information provided by the EOS survey results represents a collective summary of EOS perception in the industry. It also clearly identifies the most common important issues and observations. At the same time, the information reveals that a better industry-wide understanding is still needed to address EOS issues. It is helpful to keep in mind that while the information from the

survey results may not address everything, it certainly points to the directions that should be considered.

First we summarize some generally accepted findings from the survey:

- EOS is the most common attribute of reported returns.
- The vast majority of respondents indicate that "damage signature" is used to determine EOS.
- EOS almost always represents permanent damage.

These observations alone suggest that, as expected by many in the industry, EOS is an industry wide issue (affecting supplier and customer operations in system / component development) that needs to be addressed. It is informative to list the top four root causes of failures exhibiting EOS damage as discerned from the survey.

1. **Misapplication**: Misapplication (referred to as power handling in Chapter 4) stands out as the most widely reported root cause, involving a significant (over 20%) percentage of the reported failures exhibiting EOS damage. Misapplication can include unintended overvoltage, power supply sequencing, poor insertion (wrong orientation, misaligned devices), as well as incorrect biasing during applications.

2. **Absolute Maximum Rating:** A number of failures exhibiting EOS damage were attributed to applied voltages exceeding a specified AMR voltage. It is recognized that without proper AMR information on the datasheets, the likelihood of EOS damage increases. AMR are important for all applications that are utilized by the suppliers, manufacturers, and OEMs. It is important to note that a clear comprehensive definition of AMR becomes critical for effectively addressing EOS caused by misapplication.

3. **ESD Related**: Although it has been clearly established that component ESD target levels are not related to the rate of EOS damage, other forms of ESD have been observed at the system level and reported to contribute to the conditions causing EOS. These include charged board or charged cable events, system level events, discharges from charged devices, and ESD controls in manufacturing which are not compliant with handling ESDS devices. All of these events can be mitigated to a certain degree by paying close attention to, and improving ESD control practices, and ensuring that the levels of ESD control are appropriate for the devices, circuit boards, modules or products being handled.

4. **Miscellaneous Causes**: Beyond misapplication, AMR and ESD, many causes have been noted. As expected, these miscellaneous other reasons range from weak PCB designs to mishandling. Although each individual damage mode in this miscellaneous class is not widely reported, they do represent EOS root causes in their own right.

While these observations are all important, it is also useful to note the confidence levels regarding methods addressing these failures which exhibit EOS damage. These levels are listed below.

i) **Root Cause Identification.** The survey results give the impression that most respondents are confident in tracing the root cause and confident that damage signatures from properly conducted FA reports can provide a *critical link* towards diagnosis of root cause.

ii) **Communication**. The lack of information on conditions at the time of EOS damage can result in misdiagnosis of root causes, and can quite often result in ineffective or insufficient EOS prevention solutions. One effective way to address this is to clearly document the environmental and electrical conditions of applications in the 8D reports. Most feel confident that these would be very helpful. Including the AMR information in the communication process can go a long way to increase this confidence.

2.4 Impact of EOS Damage

It is clear that EOS has a large negative impact on the electronics industry. It is a primary, if not the top cause, of component returns at most companies. It was shown in the survey (see Figure 8) that the fraction of failures resulting from EOS damage among all failures ranged from 0% to 80%, with an average of about 25%.

It was further shown that the majority of damage was occurring not during component manufacturing, but in PCB/module assembly (30% on average) or in field applications (40% on average). As described earlier, component failures at these later stages can be very expensive, both in resolution time and cost. In most high reliability applications, if the failing devices in the board or product can be accessed, the devices are returned to the device manufacturer where resources are used to diagnose the failure and attempt to determine root cause. Failures exhibiting EOS damage during development or qualification of a new system can delay the entire program while the failure mechanism is found and an effective solution is found and implemented.

Failures resulting from EOS damage in the field are particularly troublesome. This is where the EOS impact is most keenly felt among multiple stake owners in the production chain. This is also where the potential for incorrect information or incorrect diagnosis about what actually happened becomes most troublesome. Often during the process a “discovery” may be found, and all parties are quick to put a “containment” fix in place and conclude victory, but the root cause of the underlying EOS issue may be left undiscovered. Care must be taken to analyze all potential locations where conditions leading to EOS can occur through a “fishbone” diagram that can involve multiple production facilities. “Maps” of where the damage can occur must be carefully tracked and updated, with severities noted, as both the energy levels and locations can give clues as to where the energy is coming from.

Communication among all parties is critical. The key is to share information and view the investigation, discovery and solution process as necessary opportunities for improvement and not to place blame. Often the solution can be a fix that is not EOS-related. That possibility must always be taken into account. The next section will describe a method for stakeholder interaction through the use of failure reports. Chapters 4 and 5 in this white paper give a number of examples of EOS investigations involving the entire supply chain and provide an illustration of good methodologies for EOS investigation and successful improvement.

2.5 Failure Reports of Products Exhibiting EOS Damage

There is perennial confusion in distinguishing and classifying failures resulting from EOS damage with those resulting from ESD events through FA reports. Simply classifying them as "EOS/ESD" is not helpful and mistakenly gives the impression that EOS and ESD are one and the same, which they are not. As most companies have indicated in the survey, the most effective manner to address failures resulting from EOS damage is through detailed analysis and identification of the true root cause. Therefore, FA reports can play a critical role as long as the conclusions are not misleading to the customer or to the supplier. It has been noted that EOS damage can occur in different locations on the chip, or within multiple components of a system, and so it can be difficult to pinpoint a root cause. For example, a latent defect in a very high yield process which, when present, may lower the breakdown voltage of a path such that operation over time changes a latent defect to failure. The failure may manifest as looking like ESD damage when in fact it was not subject to an event exceeding AMR at all. Careful failure analysis and communication between supplier and customer regarding device operating conditions can make the difference between a diagnosis of EOS from ESD and a process defect driven diagnosis which is not EOS.

The information from FA reports can lead to the creation of EOS-related 8D report “formats” that a majority of customers would like to see. The survey results indicated that the 8D reports serve an important function in the EOS analysis. It does not mean, however, that this directly relates to EOS. But it does indicate that following the 8D process could help reduce the incidences of EOS.

FA reports can fall into two categories: 1) reports with a well-defined damage mechanism and 2) reports with unknown conclusions. If a report shows a systematic failure mechanism in each case (or device after device), there is a clear case for finding the root cause and for fixing the problem. Finding the root cause should be the ultimate goal of the 8D report. But if the FA indicates detection of one random failure, never to be seen again, then writing the 8D report will very likely fall short of this goal. Thus, an overall balance between FA report results, documentation of the 8D reports to communicate the cause of the problem, recommendations to resolve them, and improved communication along these lines, could help to mitigate EOS.

Chapter 3: The Definition of EOS – Finding Common Understanding

David Klein, Synaptics
Robert Ashton, ON Semiconductor
Harald Gossner, Intel
Jean-Luc Lefebvre, Presto
Christoph Thienel, Bosch
Terry Welsher, Dangelmayer Associates

3.0 Introduction

The purpose of this chapter is to provide a practical interpretation of EOS using information commonly provided in datasheets: the AMR. This definition is essential for further discussion in this paper and is crucial for communication between suppliers and customers. Past experience shows that misunderstanding EOS can lead to disastrous results. An aligned understanding allows semiconductor manufacturers to clearly provide the maximum electrical limits for their devices. Knowing these limits allows system manufacturers to optimally incorporate those devices into their systems while providing a working environment in which the devices can safely operate.

During discussions to define EOS, it became obvious that there are many interpretations. While they often share some basic characteristics, the details of these definitions vary. For example, some definitions recognize the time dependency of the electrical stress; others are adamant that EOS is a DC or near DC phenomenon. To further complicate a single EOS definition, these many definitions are not held lightly by their advocates. Not only do the definitions have economic consequences, but they frequently represent years of hard work and effort and, as a result, are often fiercely defended.

Many kinds of situations can cause an electrical device to operate outside its intended electrical range. Whether these conditions are caused by its environment, happen during testing, or occur during regular operation, a critical distinction must be made: has the device reached the level of an EOS event or is it still below the specified maximum operating condition of the system or device? It is well known that brief operation above the specified maximum operating condition may not result in immediate failure, even though this operation will stress the device and may decrease its lifetime. Increasing the stress condition further then leads to immediate damage in the same device or device region where the initial stress was seen. The essential requirement is to provide limits to electrical parameters for electrical devices describing when they begin to be exposed to EOS.

To reach a common understanding which more precisely describes the situation of electrical overstress, a differentiation has to be accepted between an EOS event, EOS damage, and an EOS root cause. An **EOS event** is notable when it results in disruption of normal system operation, particularly if the device is permanently damaged. This is called a **failure related to EOS damage**. However, damage can still occur in a system that remains functional, only showing up as a reduction in the device lifetime.

Similarly, a clear definition of EOS should aid in the analysis of failures which exhibit EOS damage by providing common ground for categorizing the actual **root cause of the EOS**. It is necessary to

be able to correctly categorize the root cause in order to debug, correct, and optimize systems to protect against EOS (as discussed in Chapter 4).

Taking into account the broad understanding of the phenomenon, the following definition of EOS is presented and will be used as the basis of all discussion in this white paper:

> *An electrical device suffers electrical overstress when a maximum limit for either the voltage across, the current through, or the power dissipated in the device is exceeded and causes immediate damage or malfunction, or latent damage resulting in an unpredictable reduction of its lifetime.*

Critical to this definition is a clear understanding of what is meant by maximum limit. The rest of this chapter will further expand this definition by providing a practical interpretation of EOS in terms of AMR, looking at existing, accepted documentation practices to bring color and life to our definition.

3.1 Existing Documentation Practices of AMR Values

The purpose of this section is to look at different uses of AMR across the industry to describe the maximum limits of operation which should never be exceeded. Examination of existing documentation shows that different manufacturers have their own unique ways of defining an AMR for a semiconductor component.

One use of AMR can be found at JEDEC. Here it is defined as the maximum voltage that may be applied to a device, beyond which damage (latent or otherwise) may occur. However, absolute maximum ratings can refer to voltage, temperature, currents and any other operation parameter which can cause damage to the device.

Similarly, some industry references indicate that stresses above absolute maximum ratings may cause permanent damage to the device [1-4]. It is emphasized that this is a stress rating only and functional operation at this or any other conditions above the specified operation conditions is not implied. Exposure to absolute maximum ratings for extended periods may affect device reliability. Due to the statistical nature of destructive fails, any AMR level needs to be related to an acceptable failure-in-time (FIT) value. However, in general, no details on failure rates are provided with AMR tables in datasheets. Similarly, the specification of unique destruction levels for short duration stress is not evident due to the time dependence of the damage mechanisms.

Insight into the electrical aspects of AMR can be gained by examining the voltage ranges illustrated in Figure 21. First, there is the safe operating area, a region of robust operation (region A). This is the region in which the manufacturer designed the device to operate. This is followed by a region in which operating restrictions exist (region B). In region B, the device is not guaranteed to function as specified, however the device is not expected to be physically damaged. Operating the device in region B for extended periods of time may also result in reliability issues. The upper limit of region B is the AMR. At and beyond the AMR the user should expect problems. Beyond the AMR are two regions of electrical overstress with either latent (region C) or immediate (region D) damage as a result of exceeding AMR. Note that the transition between latent damage and immediate damage is subject to normal process variations as illustrated by the yellow S curve starting at the high end of

region C. In order to properly evaluate the product reliability and robustness, it is important to understand that some qualification stresses, such as device level ESD and latch-up, are *expected* to run evaluations that will exceed AMR. For example, in the case of latch-up, this may be necessary in order to get significant current injection to assess latch-up robustness. Regardless, a device operating in either region C or region D is experiencing EOS.

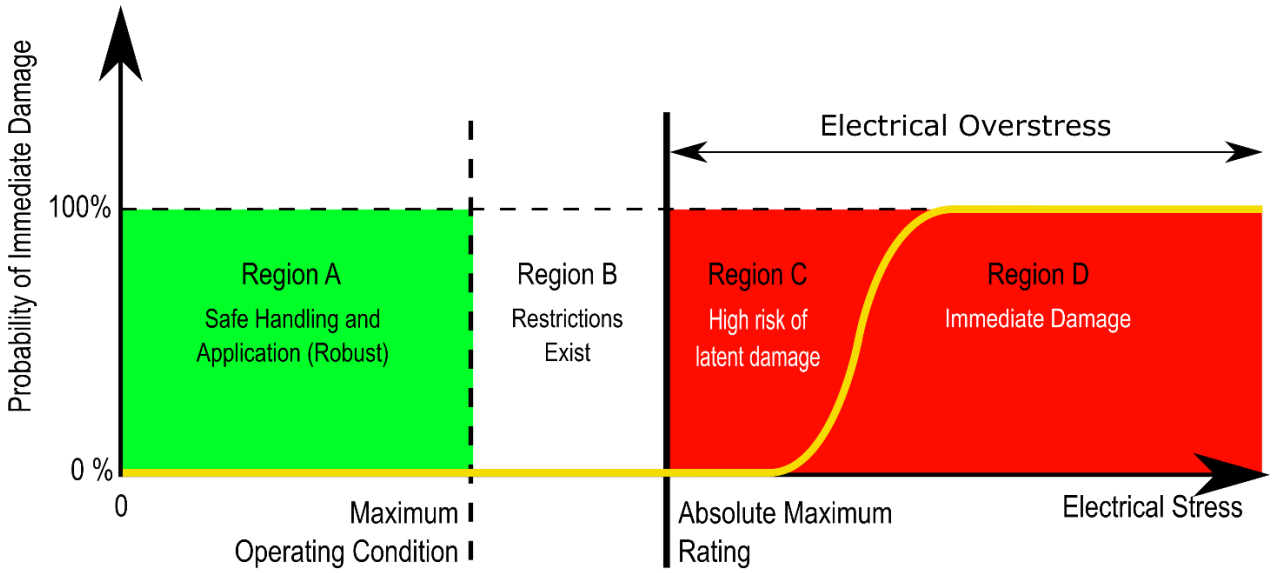


Figure 21: A graphical depiction of how Absolute Maximum Ratings should be interpreted. The yellow line is the number of components suffering immediate, catastrophic EOS damage (repeated from Figure 1).

In addition to the electrical and ambient conditions that the AMR values are based on, there are differences in the way stress data is assessed when the AMR values are being extracted.

- Region C:
  A manufacturer may pick conservative AMR values not based on physical properties of the product. This results in a wider region C before the onset of immediate damage. Alternatively, the manufacturer may define the AMR values based on detailed circuit and technology understanding for an accurate prediction of the damage threshold. This detailed approach would result in the yellow S curve in Figure 21 shifting left until the point where it rises up from the X axis while nearly touching the AMR boundary, greatly reducing region C. Regardless of the method chosen, the manufacturer is *solely* responsible for defining the AMR values.

- Time dependence:
  The AMR may be defined by a single voltage or current or it may have different values for different stress durations. Ideally, any documented value should have a fixed time association.

In general, the astute system manufacturer should understand that while an operating region may exist between the specified maximum operating condition and the AMR values (region B), this region is there to provide a buffer for stress events to the system without disrupting normal

operation. The device is typically not tested or guaranteed to be fully functional above the specified maximum operating conditions. Any attempt to operate in this region must be discussed with and agreed upon with the supplier. Additionally, not every device will fail immediately upon experiencing an event above AMR (region C). However, this is still an EOS event and is considered high risk for latent damage and likely future permanent damage. Any unit experiencing an event exceeding AMR will have the risk of experiencing latent EOS damage. Finally, a well written AMR will often be specific to the environment in which the device is expected to operate by its manufacturer. It is not only the manufacturer's definition of the maximum electrical and thermal limits, it also defines the limits of the manufacturer's responsibility when the component is damaged as a result of exceeding those limits.

Beyond this discussion of regions of operation where the AMR describes maximum electrical and environmental values of operation, there is controversy about whether it should also refer to ESD limits. As noted above, while recognizing that this definition of EOS focuses attention on the AMR, placing greater significance and expectations on its limits than may have been given in the past, each supplier has their own approach to setting the AMR values. With respect to ESD, several different approaches have been observed:

- Some suppliers do not include ESD limits as part of their AMR because testing to establish the ESD limits often does not have similar statistical data collected as is required for setting more traditional items such as voltage.
- Some suppliers do place ESD limits in their AMR definition as it is felt that this is part of the overall agreement that must be met between supplier and customer.
- Other suppliers have placed ESD limits in an AMR section for no other reason than it was the only place that it made sense to them.

Regardless of the approach taken, the supplier is *solely* responsible for deciding what parameters and limits are included in their product's AMR.

Careful understanding of the AMR by a system manufacturer is necessary to ensure that the operating environment of the system is within the specified operating conditions given by the device manufacturer and the limits defined in the AMR are never exceeded. This is particularly important if the system is using the semiconductor device in new or unique configurations. Here, communication between the semiconductor supplier and system manufacturer is absolutely necessary, particularly if the AMR does not appear to cover modes of operation that the system manufacturer expects their system to experience.

Finally, the authors recognize that this definition of EOS focuses attention on the AMR, placing greater significance and expectations on its values than may have been given in the past. Since this is a new interpretation of existing documentation, system manufacturers are encouraged to communicate with their suppliers and verify AMR values in any datasheet published prior to release of this white paper to confirm that the AMR values follow this new interpretation.

3.2 Unified Understanding of AMR and EOS

The following criteria are proposed for a consistent terminology of AMR across the industry, which are also applied in the rest of the document:

- AMR specify the constraints for excursions in system operation and environmental conditions which need to be met by system design to allow safe operation and handling of semiconductor components.
- The electrical and environmental conditions for which the AMR values are intended have to be documented in the datasheet. The data assessment leading to the documented AMR values is at the supplier's discretion and responsibility.
- In systems with unique requirements, the values of AMR have to be provided by the semiconductor component supplier according to the electrical and environmental conditions given by the system manufacturer.
- To facilitate the test and communication of AMR aspects, standardized stress test methods, as far as possible, should be used.
- An EOS event occurs if any AMR is exceeded for any period of time.

3.3 Additional Comments on Usage of the Term "EOS"

The definition for EOS presented in Section 3.0 has been chosen by the authors of this white paper as the most practical and clear approach for this document and for communication between suppliers and users of electronic devices. It is important to note that in the broader electronics industry, the term "EOS" will be used in other ways:

1. Failure analysis engineers are likely to assign, some would say prematurely, the term EOS to any visible damage that appears to have been the result of excessive voltage or current. These assignments are often based on experience and may often be correct. However, the FA engineer often makes this assignment without knowledge of the maximum limits of operation or any information on the real world electrical event and therefore does not know whether the device experienced EOS per our chosen definition. The FA engineer may argue that any device that is charred, burned or partially vaporized very likely has been "overstressed". It is understood that there is a large community of FA engineers who will use "EOS" this way in spite of attempts here to drive towards a common language.

   To that extent, this white paper introduces the term "electrically induced physical damage" (EIPD) to represent the term that should be used by FA engineers when no clear communication has been completed with the customer as to possible root causes of the damage. The definition of EIPD is the following:

   Damage to an integrated circuit due to electrical/thermal stress beyond the level which the materials could sustain. This would include melting of silicon, fusing of metal interconnects, thermal damage to package material, fusing of bond wires and other damage caused by excess current or voltage.

   EIPD is used when it has not yet been determined if a unit experienced an EOS event by the definition in Section 3.0. That determination can only come once the supplier and customer have worked together to look at root causes.

2. There can be confusion about the relationship between EOS and ESD. ESD is merely one type of electrical stress that can exceed the specific capabilities of a device. EOS is a much broader term which contains ESD as one possible cause. It is critical to understand that EOS refers to many independent possible root causes and thus there is no one protection strategy for EOS. Because many device users seem to be confused by this, it must be stated clearly, *ESD protection does not provide protection for all EOS root causes*. Because of this confusion, some have suggested that any definition of EOS should explicitly exclude ESD; this is not our intent. The purpose of this white paper is to address all root causes of EOS damage, including EOS damage due to ESD.

3. There is disagreement on the statement that "there is no EOS event until the device has been damaged". Instead, it is argued that once a specification maximum limit has been exceeded, there has been, by definition, an "overstress". The user is fortunate that the device still operates. Again, the definition we have chosen comes from a practical consideration: it is only devices which have been damaged that are ultimately returned to the supplier. So again the definition is tuned to the main problem in the industry – the unacceptably high rate of returns due to damage from EOS root causes.

3.4 Conclusion

This chapter has provided insight into the diverse and divergent use of the terms EOS and absolute maximum ratings in industry. This diversity is a large concern and is a root cause for many reported fails in the industry. To remove this obstacle and enable a consistent and reliable design flow from IC to system, a unified definition of AMR and EOS has been presented, using the most common understanding of AMR and EOS. This is not an abrupt break with existing industry practice but rather allows a convergence into more precise use of the terms and better alignment between semiconductor suppliers and system customers.

References

[1] Analog Devices Technical Article MS-2251, http://www.analog.com/media/en/technical-documentation/technical-articles/MS-2251.pdf

[2] Operating Requirements for Altera Devices, https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/ds/dsoprq.pdf

[3] Handling Precautions DS00-00004-2E, http://www.fujitsu.com/cn/Images/readme5.pdf

[4] Honeywell Technical Note, http://sensing.honeywell.com/pressure%20sensor%20glossary%20of%20terms_tn_008200-2-en_final_08jul11.pdf

Chapter 4: EOS Root Causes

Harald Gossner, Intel Mobile Communications
Fred Bahrenberg, Dell
Jeff Dunnihoo, Pragma Design
Pasi Tamminen, Microsoft Corporation
Christoph Thienel, Bosch

4.0 Purpose

Chapter 4 provides a terminology of categories and subcategories for EOS root causes. It also highlights the common ways of analyzing EOS damage. This terminology is used throughout the rest of the document.

Three basic categories for the root cause of electrical overstress are identified:

1) Unpowered handling
2) Powered handling
3) AC operation or switching

Each of these categories can further be divided into subcategories (for example, hot plugging-related misapplications or testing-related misapplications). An overview of these root causes are presented in Section 4.1 and the main categories are then discussed in Sections 4.2 through 4.4.

During the analysis of an EOS problem, it is very important to describe and quantify the problem adequately. Typical ways of analyzing EOS damage are:

1) Observation and empirical description of the occurrence and analysis of the physical signature of the damaged part → What?
2) Reproduction of electrical failure mechanism and analysis of the stress paths → How?
3) Root cause detection by a quantitative assessment of the real world situation and the interaction between the stress source and the damaged part → Why?

A more detailed consideration of the above will be discussed in Section 4.5.

4.1 Root Cause Categories

Electrical overstress can be caused by a wide variety of root causes. A concise, *but not exhaustive*, overview of them is shown in the fishbone diagram in Figure 22. The main branches are unpowered handling, powered handling and AC operation/switching related root causes. Each of them can be traced to a more specific subcategory. Typically, it is only at this subcategory level that the formulation of an appropriate description of the root cause and corrective action can be completed. It should be noted that it is not typically possible to achieve better robustness in one failure category by improving the robustness in another category, e.g. there is no improvement in hot plugging

related fails by increasing ESD robustness. In some cases, hardening for one failure model can even be counter-productive for another failure mechanism. This requires a clear analysis of an EOS problem and the related design measures. Critical information on the causes for EOS can be gathered by carrying out line walks and application studies in the field and are necessary to determine root cause.

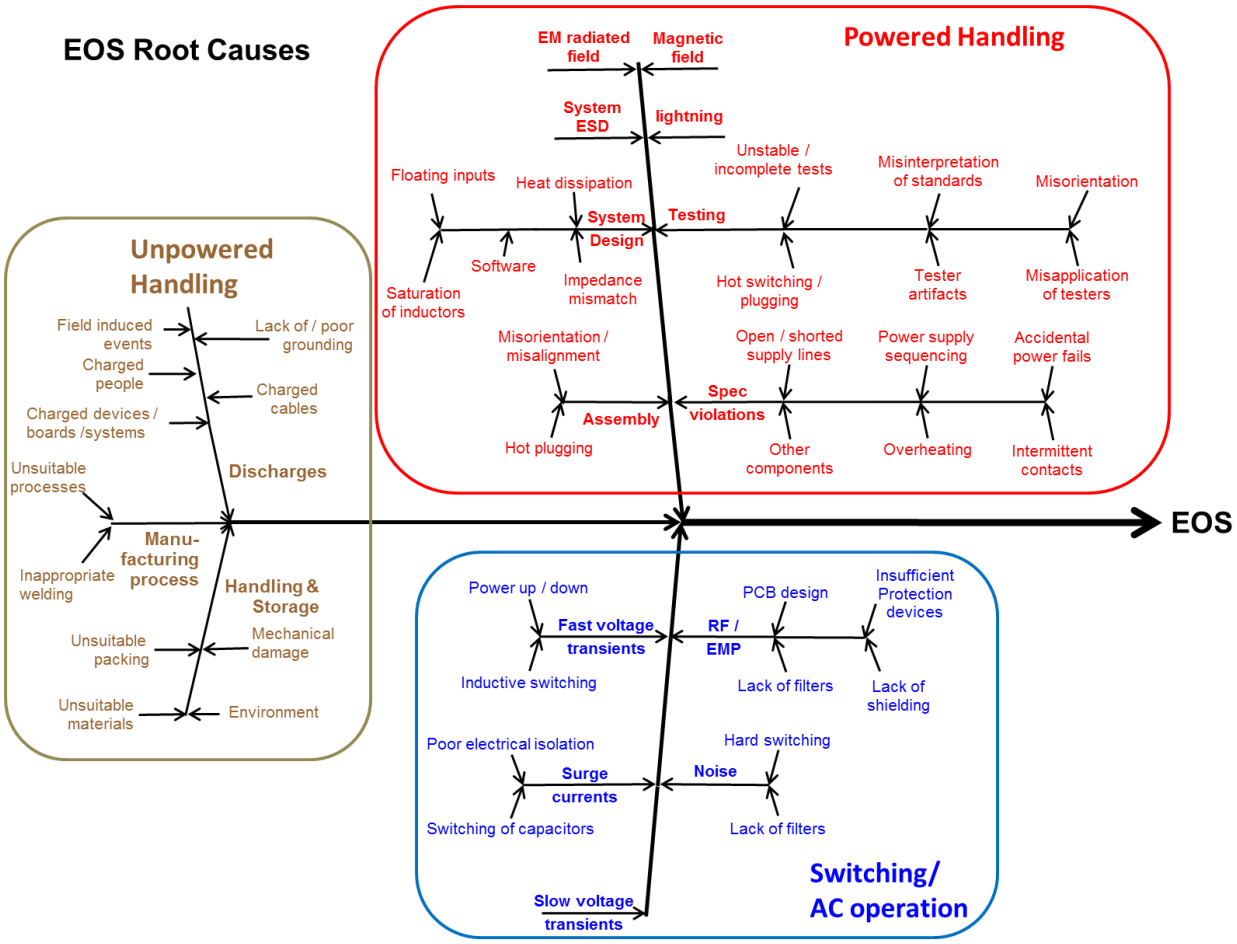


Figure 22: Fish Bone Diagram Indicating Categories and Typical Subcategories of the Root Causes for EOS Damage (the sub-categories are not an exhaustive list, repeated from Figure 2)

4.2 EOS Damage during Unpowered Handling

There is no simple way to classify EOS events due to any discharge as there is a wide bandwidth of events. ESD itself is fairly easy to model by tracking the current versus time of the event. The current waveform can be further examined by specifying the pulse rise time, peak current, polarity, charge transfer, energy transfer, power dissipation, oscillation frequencies and duration. Unfortunately, these parameters are valid only at the point in time when the discharge occurs and changing just one of them can produce different device/system responses. These parameters are also highly dependent on the environment and the product itself, making it challenging to repeat any real life ESD event. Therefore many of the identified and reported real life ESD cases are from manufacturing where the environment and processes are under better control.

The classification of ESD events are CDM and HBM discharge scenarios at the device level, and CDE, CBE and human metal model (HMM) at the system level. Actual real world discharge current waveforms (such as the examples in Chapter 5) are case specific, with little similarities to standardized HBM, CDM or IEC 61000-4-2 waveforms. Nevertheless, standard ESD waveforms are able to reproduce similar failure signatures. Therefore, we can use CDM to represent fast, short device level ESD events and HBM to represent slow, long and lower current events. At the system level, CDE and CBE represent the common real life events and HMM represents a scenario where a high current pulse is followed by a lower amplitude residual pulse.

These ESD cases are presented in Table 2. The waveforms have some typical signatures; energy source, rise time, peak current, energy and power levels. In addition, there is information about the defect signature, occurrence and event probability.

Table 2: Overview of Typical ESD Discharge Events with their Key Parameters.

		Waveform parameters				Defect Signature		Occurrance / Situation	Real life probability
Waveform	Energy source	Rise time [ns]	Peak Current	Energy content	Power	Damage area	Melted area		
CDM	Internal	<0.1	<20 A	Low	High	Small	Rare	Wafer mfg., Device testing, Back end process	High
HBM	External	>2	<10	Medium	Medium	Small / Regional	Sometimes	Manual handling of devices without EPA	Rare
CDE	Internal / External	>0.2	<50	Medium / High	Medium / High	Small / Regional	Sometimes	Cable attachment events	High
CBE	Internal / External	>0.2	<50	Medium / High	Medium / High	Small / Regional	Common	Cable attachment events, system handling	High
HMM	Internal / External	>1	<35	Medium / High	Medium / High	Small / Regional	Common	Touching system with a metal tool	Rare

While electrical stress during unpowered handling is part of an EOS root cause, there is commonly a differentiation between ESD and other EOS types of damage. This is of practical importance, because protection against ESD events during handling of non-assembled IC semiconductor devices has to be implemented as on-chip protection circuits, which can only handle relatively low energies due to the very small dimensions in semiconductor technology. It is a widely applied approach to use failure analysis methods to find the physical damage on chip and relate the detected failure signature either to an ESD event or to other EOS-type damage. In this context, there is a common misconception that high ESD robustness according to HBM and CDM helps to increase the general EOS robustness of the system. This is not correct, as shown in various examples in Chapter 5, and leads to misguided optimization strategies. While ESD describes a specific stress situation, EOS is a result of exceeding an AMR value which can be due to a wide range of root causes (see Figure 22). As a result, the idea of increasing ESD robustness to avoid EOS is not a valid approach, see Figure 23.

→ EOS	***Amount*** of stress (spec was exceeded)	***quantity*** of stress
→ ESD	***Kind*** of stress (discharging of C)	***quality*** of stress

→ EOS and ESD are ***not alternatives*** to each other; ESD can be ***a cause*** of EOS damage

Figure 23: Relationship of EOS and ESD

A specific type of EOS damage related to ESD is a subsequent fail when the system has been powered on. This is due to the fact that while ESD damage may only cause marginal damage to the integrated circuit, subsequent application of power to the circuit may result in concentrated current at the site of the ESD damage which can result in localized heating and subsequent damage or may trigger a latch-up event.

Another often heard concern is latent fails due to ESD damage during manufacturing which could lead to massive EOS damage even when the system is respecting AMR conditions. While there are few reports on latent fails at stress levels close to the ESD failing levels of a device [1], a clear relation of EOS field fails to latent ESD damage has not been reported. One reason is that ESD handling controls for ICs are very efficient and the typical qualification goals for ICs of 1 kV HBM and 250 V CDM guarantee enough margin to avoid latent fails [2,3].

An effective ESD control program **avoids charging or fast discharging** in the assembly line. A wide range of factors have to be considered here: floor, shoes, stores, transportation boxes, system chassis, conveyors (shown in Figure 24) and plastic material assembled to the end-customer system such as in a car.

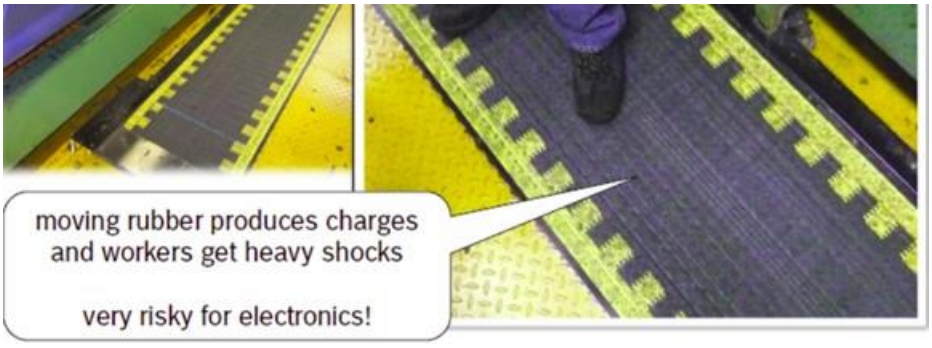


Figure 24: Conveyor ESD Risk in an Assembly Line

Appropriate measures are well established and described in various Industry standards [4]. Not paying attention to these measures results in a significant number of fails and yield loss. Therefore, every electronic manufacturing line handling semiconductor devices has to be aware of this and must follow ESD control methods.

However, there is an increasing challenge in the Industry. In the past, systems were built in dissipative enclosures that could be grounded via a bench or conveyer surface during the assembly process. Today, electronics are placed into insulated plastics, or painted enclosures, which prohibit the electronics from being properly grounded during the assembly process. Ensuring these plastic parts have not charged up the electronics is a major challenge during system assembly and field service operations.

Another example of the occurrence of EOS during manufacturing is electric welding. Welding is a very common manufacturing technique for the automotive industry. Light trucks are often upgraded with extra equipment by specialized companies. Many of these companies don´t follow EOS protection strategies such as ensuring a short welding current path by keeping the ground contact close to the welding point (see Figure 25). This results in high currents across the vehicle and possible damage to the vehicle electronics.

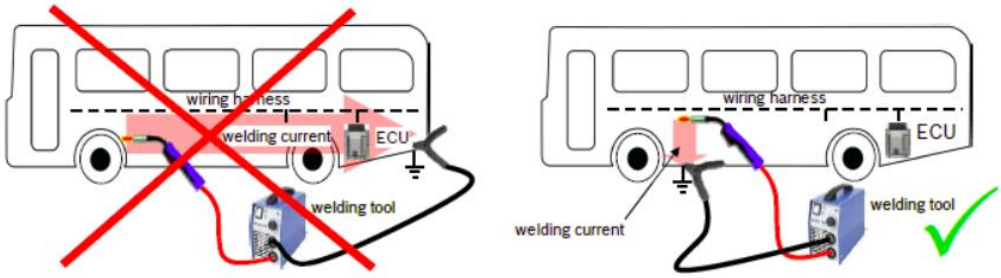


Figure 25: Proper Grounding of Welding Tools to avoid Electronics Damage

In addition, the quality of the ground contact has a big influence on the stress to the electronic control unit (ECU). The lower the resistance is, the cleaner the welding voltage. Any paint, dirt, or rust may increase this resistance, resulting in large voltage peaks during the welding process in order to maintain the chosen welding current.

4.3 EOS during Powered Handling

EOS damage during powered handling is split into very diverse branches of root cause subcategories. This section will discuss just a few; hot plugging, system level ESD and misuse versus system design weakness as examples.

4.3.1 Hot Plugging Related

According to the induction law, a voltage will be generated if a current in a solenoid is interrupted (or ramped) fast enough. For example, such solenoids and wires (which are also solenoids) can be found in a large number of modern cars. Hot plugging (or unplugging) means to change a current in an abrupt manner, regardless of whether it is intended or not. Under “hot” conditions, each opening of contacts means a change of a current and thus may generate risky induction voltages. Because of

intermittent contact pins inside the connector, this could happen many times during one connecting procedure, introducing even more risk.

Hot plugging happens in a large number of applications every day. An example is taken from the automotive industry and describes the situation representatively for other applications. In the automotive industry, hot plugging is very common, because it is unavoidable. After switching off a car ignition, power, being directly supplied from the battery, is still needed for several minutes for safety and comfort applications. If any plugging or unplugging event occurs during this period of time, it is unknown whether the power connection is still supplied. If it is, the plugging procedure may generate induction voltages through current change. Hot plugging can generate bursts of voltage peaks which may be transported to any car components via the wiring harness. The result can be that hot plugging to one part of the car may destroy an electronic device at the other end of the car and result in EOS damage.

In order to avoid EOS damage by hot plugging, many industries successfully prepare their connectors by first-mate-last-break (FMLB) grounding contacts just by extending the ground contact pins. During hot plugging, the ground contact now mates first and during unplugging it breaks last, thus ensuring a 100% reliable ground potential reference. In the case of hot plugging, the power is always guided to its target path. However, if the FMLB feature is missing, and if there is no accidental ground connection by the standard ground contact, the power is forced to find alternative paths at the beginning or at the end of the hot plugging procedure. In this situation, it cannot be predicted which device or component may be destroyed, but possible damage depends on the strength of overstress and robustness of all involved devices. However, it should not be concluded that there are weaknesses in the destroyed devices as the root cause is the hot plugging procedure itself, assuming those voltage peaks exceeded the product AMR.

Up till now, FMLB is not standard in the automotive industry, except for onboard diagnosis connectors. The lack of a FMLB therefore makes hot plugging very risky in the automotive industry. Unintended hot plugging happens during automotive assembly, operation, maintenance, and repair as illustrated by these examples:

- A worker does not realize a car has voltage applied while they are assembling devices into the car (ECUs, doors, seats, windows, etc.).
- During “failure isolation”, components are removed and exchanged in a powered system.
- Loose contacts: battery charging is interrupted by unfixed connectors (a scenario known as load dump); broken contacts in the test adaptation for the ECU; moving a power supply in a car maker`s line which has loose contacts.
- Prior damage to wiring in a harness creates interruptions in an uncontrolled way during operation of the car.

As shown in Figure 26, switching off the ignition of a car does not mean the current in the car is also off. Several applications in the car are still actively supplied directly from the battery’s positive terminal (terminal 30 as per DIN 72552). For several minutes there are amps of current, decreasing over time down to milliamperes.

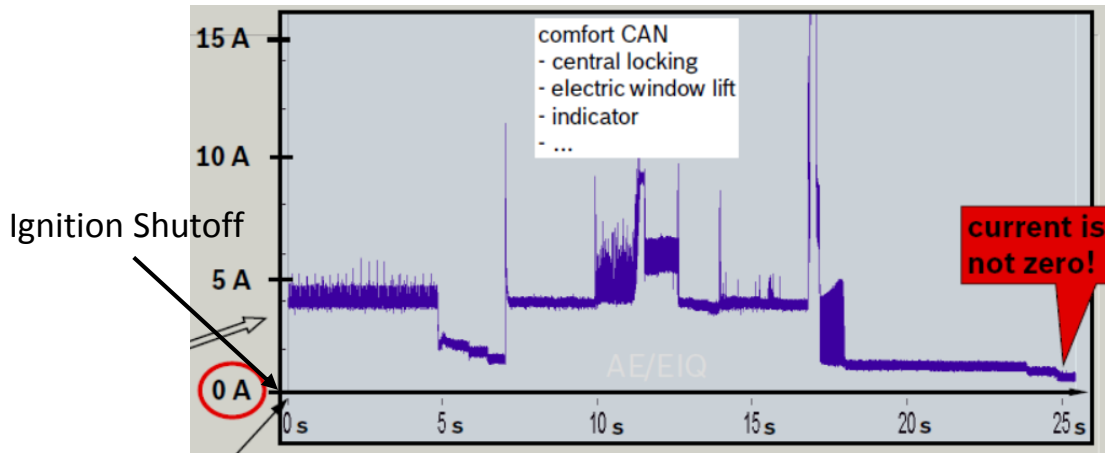


Figure 26: Residual Current after Ignition Shutoff

During the automotive assembly process, sometimes an external power supply is necessary, since there is no battery on board yet. For example, this is the case when electric power seats or power windows are assembled. Power is needed in order to move the parts for fixing some screws. Sometimes this external power is applied hot in order to save the time required for switching on and off the power. Therefore, during the assembly process, the car experiences several hot plugging events, some of which may cause overstress.

An example of massive overstress due to intermitting contacts was found in a manufacturing line of engines when a diesel truck engine was started for the first time. An external power supply was connected to the screws of the starter by 50 m long wires, which were manually held to the threads of the screws during the starting process.

This unsafe connection caused huge starting currents to be switched off and on, generating a burst of out-of-specification induction voltage peaks. These voltage peaks destroyed the diesel injection electronics, including the heavy copper cables, see Figure 27.

Figure 27: Example of Improper Contacts during Engine Start Up

In a third example, a worker in an automotive assembly line customer installed the battery into the car. The positive pole was attached to the terminal and the negative (minus) pole was left unattached in order to keep the car unpowered. But the final ground wire from terminal to chassis was too stiff, pushing the contact shoe back to the minus terminal of battery and creating a loose contact with it as shown in Figure 28.

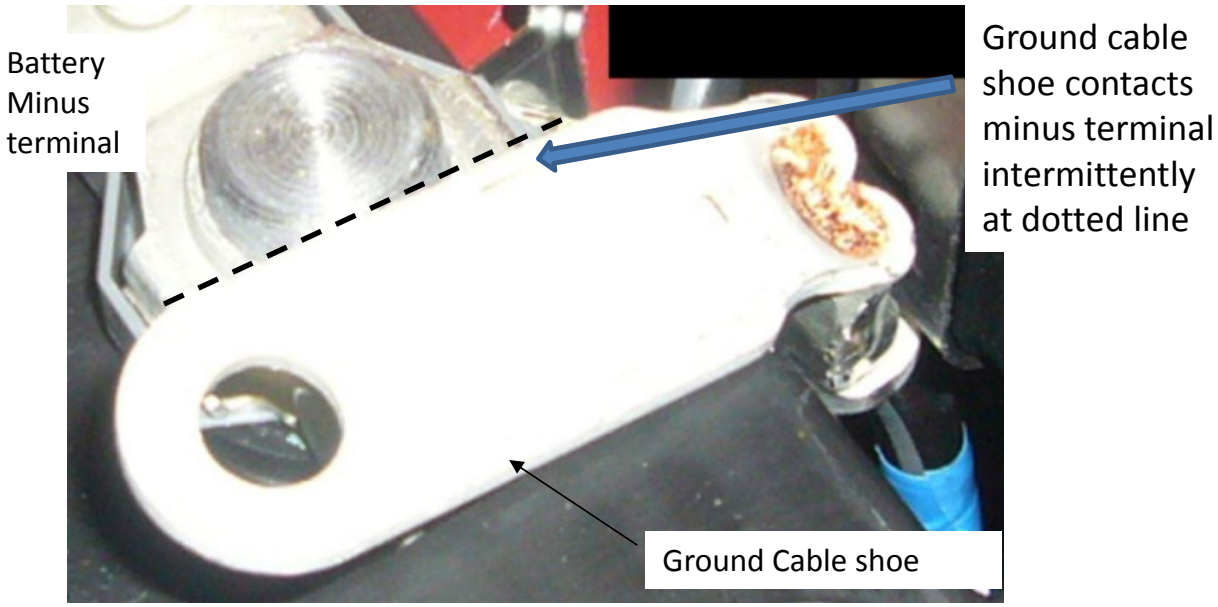


Figure 28: Interruption of Battery Contact during Assembly

The resulting battery contact left the car powered and all work inside the car was potentially hot plugged. By moving the car during the assembly process, the contact was opened and closed multiple times. This also created a burst of inductive voltage peaks damaging electrical components in the car being assembled.

In another case, a car´s battery was charged as the car moved through the assembly line of the automotive manufacturer by a mobile external power supply. The positive charging cable didn't have any cable strain-relief between the car and supply. As a result, the supply was torn from the moving car via the positive charging cable. From time to time, this unsafe construction resulted in a pulling force which unplugged the positive clamp from the battery terminal and interrupted a very large charging current, creating huge induction voltage peaks which resulted in damage to sometimes one or more ECUs.

In a final example of contact issues, for cost savings reasons, a test adapter for an ECU test in the assembly line of an automotive manufacturer was not regularly maintained. As a consequence, it was possible for broken contact needles to go unnoticed. These contact needles were used to make connections to the ECU power. Alternatively, these contact needles could have a build-up of dirt on the contact surface of the needle, resulting in less than a fully operational connection. As a result of this improper maintenance, contact needles made either poor contact or no contact at all during the inline 100% test of the ECU. This led to interruptions in power tests of the ECU and damaged many

ECUs. In this case, something as simple as a lack of general maintenance resulted in a significant number of ECUs having EOS damage.

EOS issues can also appear at end-customer use due to latent damage in assembly. During automotive manufacturing, wires can be pulled through narrow cuts inside the car chassis with strong forces, workers might stand on wires crossing sharp edges or workers and trolleys can step on or roll over wires lying on the ground. In these cases, some wires or connectors might mechanically be overstressed leading to a subsequent break in the terminal contact after the car has been driven long distances without any sign of a problem. These intermittent contacts can result in EOS damage.

4.3.2 System Level ESD Related EOS

System level ESD is a discharge event which occurs mostly during end-customer operation. The typical failure is a soft fail which can be recovered by the system itself or by the operator. In rare cases an excessive ESD discharge level of tens of amps can generate physical damage. The latter is considered an EOS event if it exceeds the specified levels for which the system has been designed and qualified. The qualification test is based on IEC 61000-4-2 with system specific implementation procedures described by application specific standards (automotive: ISO 10605, avionic DO-160, etc.).

System level ESD design leverages a great deal on past design experience and pass/fail testing results to determine which ESD protection measures to incorporate into new system designs. Designers add ESD protective devices to the board to prevent ESD damage at IO ports and external openings in the systems shielding. These ESD suppression devices may or may not be populated based on the outcome of the test done at the system level. If the system passes IEC 61000-4-2 with the devices populated they are removed to see whether the system continues to pass. If it does pass they are left off the design to reduce cost. Margin is assumed if passing results are achieved though some companies will test at higher discharge levels to ensure added ESD margin. This has been the accepted practice for many years and has served the design community well.

One of the challenges with the IEC 61000-4-2 testing is it assumes the system is always closed, on a grounded table, all peripherals connected, and the system plugged into power. This creates a very optimistic environment for ESD since it assumes everything is grounded, nothing is floating, signal pins are not exposed/tested and the system is completely closed which does not mimic the real world conditions.

Challenges occur when the environment outside and inside changes. For example, universal serial bus (USB) flash drives used to be a straight forward ESD design problem given the shielding provided via the USB connector. However, as users demanded smaller and less expensive flash drives, the ground shield in the USB flash drive connector was removed in some designs. Now any discharge from the flash drive goes directly to the pins of the USB port and bypasses the shielding. Additionally, as ESD margins inside the chips are being reduced, understanding what margins are present at the chip inputs in order to choose the right board protection is becoming increasing important to understand. However, few tools and approaches exist to enable designers to easily understand the amount of ESD margin the design contains, making it difficult to evaluate tradeoffs between the amount of ESD margin and loading, routing, speed, and cost.

Field service creates a very challenging environment where customers are asked to open up systems, reset cards, and reseat chips in order to prevent the dispatch of a trained service technician. Users

are also being asked to replace devices inside their systems with few ESD practices being followed or even supported via shipping of wrist straps with the replacement devices. Furthermore, no ESD testing is performed on open systems to understand the sensitivity levels of the electronics. This would be a very difficult task given the need to remove devices and test them for damage during each phase of the testing. It is also impractical, costly and would degrade system performance to make electronic products immune from system level ESD at all points inside of the case. The industry assumes the service person is following good ESD practices when opening up a system, which as previously mentioned, is not always the case.

Feedback to chip suppliers is mainly received from printed circuit board assembly (PCBA) manufacturing sites where the process is controlled, data is collected and easier to obtain and digest. However, field data is very difficult to use to pinpoint the source of the damage. Was the chip at fault, was the damage inflicted by an untrained operator, by the environment, or during the handling/repair of the boards at the repair facility? Are failing ICs that are being sent back for analysis to the suppliers handled with the same level of care as new devices to preserve the evidence? These challenges create a level of uncertainty about where the root cause of the problem occurred with field returned devices and thereby reduces the level of analysis performed on them.

4.3.3 Misuse vs System Design as the Root Cause of Failures Exhibiting EOS Damage

Protection against electrical overstress requires system level consideration. Sometimes compromises are needed for achieving adequate balance between protection, performance, and costs. If EOS risks are recognized in the design phase, warnings and cautions will be presented in data sheets, users' manuals and in application notes. When the failure is caused by improper usage, despite the existing warnings, the root cause is obviously misuse.

Failures caused by misuse can effectively be avoided by recognizing AMRs and by following the manufacturer's instructions and application notes. However, misuse failures cannot always be avoided completely due to the human factor. Therefore, if misinterpreted, misuse failures at the system level may be classified as a lack of protection in the system design. However, it is the responsibility of the electronic device supplier to provide an adequate specification of the use conditions to avoid misuse. The key to resolving misuse is clear communication between supplier and system manufacturer.

4.3.3.1 An Example of the System Level Failure Diagnosis of a Switching Regulator

To illustrate the problem of misuse and missing absolute maximum ratings, the following example is presented. It also shows that operational conditions are often not properly monitored, and conclusions are drawn based on the failing circuit instead of understanding the mechanism.

A field failure rate (FFR) for switching regulators in consumer products increased above the acceptable level. The power consumption of the regulator modules increased slowly, causing latent damage in a continuous operation. The root cause of the random failures was expected to be ESD because the damage was found in the ESD protection circuits of the module interconnections by an emission microscope.

A detailed ESD analysis finally excluded ESD as the root cause, but, an additional finding during the monitoring phase in ESD stress tests was that the reference voltages of the regulators were found to be higher than the nominal values. Reference voltage was controlled by software. The reference

voltages of the switching regulators were adjusted down slightly and the problem was solved. The field failure rate decreased. In this specific case the electronic component supplier had not specified absolute maximum ratings. This led to the impression at the system manufacturer that either there was a potential to increase performance or there was no need to carefully control the system. To clearly indicate a misuse by the system manufacturer or even by the end-user, the electronic component supplier has to specify absolute maximum ratings for the given operational conditions. If the system manufacturer exceeds these absolute maximum ratings during their defined system operation or operates it at very different conditions without verifying this with the electronic component supplier, a case of misuse exists.

4.4 EOS Damage during AC Operation and Switching

Coupled RF and spurious EMI can cause EOS just as readily as any directly applied current overstress. In receivers, delicate detector diodes and RF front ends are tuned to detect and amplify extremely weak signals for the rest of the system. Even with overload clamps on the system, it is possible to overdrive the detectors at the front end and permanently damage them. For example, consider a high performance radar detector designed to seek weak local oscillator emissions from a police radar gun. Directly transmitting into the microwave horn of the detector can permanently damage the detector circuitry.

Likewise, linear RF amplifiers rely on driving a matched, tuned antenna load. If this load is not connected or if an antenna is matched to the wrong band then a high voltage standing wave ratio (VSWR) can reflect a great deal of the output power of the amplifier right back into the final output stage where it must be dissipated as heat. If the amplifier cannot dissipate the power, or otherwise throttle back the output, then it may be permanently damaged.

Finally, various forms of unexpectedly induced EMI, from sources foreign to the system, may cause EOS. Natural phenomenon such as indirect lightning strikes and even solar flares can induce voltage and current excursions on long power or signal lines in power distribution and communication links. These disturbances are usually characterized by their conducted effect at the point of entry of the system, and not generally by the induced EMI event that begins the failure chain of events.

None of these induced sources need necessarily supply the overstress energy which causes the damage. While they can cause excursions beyond SOA ranges, they may also create an in-band signaling condition which cascades a fault elsewhere in the system using local power supplies to immolate components which may appear to be totally unrelated to the entry vector.

4.5 Analysis of Electrically Induced Physical Damage and Conclusions on EOS Events

Often the analysis of a potential EOS event starts with the identification of a damaged part. To determine the reason for a non-working system or component, the technical expert needs to identify the broken part in the system and perform a detailed inspection of the system, component, board and IC. An important step in the initial analysis is the fault isolation and physical failure analysis as discussed in Chapter 6. While this approach does not deliver the information of the actual root cause directly, an analysis may point to an EIPD location that could suggest a root cause such as ESD, lightning or discharge of large impedances by the extent and signature of the fail in the system, board or IC. For example, one typical EIPD signature, which suggests an EOS event as root cause,

is an extended melt area of metal routing on the IC (often on the order of >100 µm). This is an indication of a very powerful energy pulse, excluding pulses such as a low energy ESD pulse during IC handling as root cause. Knowing that dissipated energy is a function of the current through a resistance, and the time (Energy (J) = Current^2 (A) * Resistance (ohm) * Duration(s)), examples of various amounts of dissipated energy through a 1 ohm resistance as a function of the surge or stress are shown below in Table 3.

Table 3: Typical Energy Range as a Function of Various Surge or Stress Applications

Surge/Stress	Application	I peak [A]	Duration	typical range of energy*
CDM	component	3-6	0.8 ns	1 - 10 nJ
HBM	component	0.7	150 ns	100 nJ
IEC61000-4-2	system	16	120 ns	10 µJ
ISO7537:1	system	10	2 ms	100 mJ
ISO7637:5 (load dump)	system	43	40-400 ms	10 -100 J

* in 1 ohm resistance

To understand the stress situation better, the suspected type of EOS pulse can be applied to the system or to the electronic component in order to replicate the field event. The expected outcome is that generating the same physical failure signature as observed in the field might indicate the type of EOS event appearing in the field. However, there are numerous pulse waveforms which can lead to the same signature of EIPD. Even if the stress waveform is correctly reproduced, a full root cause analysis cannot be achieved yet. In some cases single events, which by themselves are harmless but which can happen in combination, may lead to an EOS event and cause damage. An example is the use of a power supply which generates overvoltage spikes in combination with board diodes with insufficient voltage clamping which could lead to EOS damage of an IC. In these cases, the observed damage cannot be pinned down to a single root cause, but an analysis of the interaction of various contributing factors must be completed.

To get to the *true* root cause, an observation of the critical parameter during the field event is required. For example, a manufacturing audit specialist who inspects a manufacturing environment can gain information regarding the handling processes which might lead to an EOS event, such as in mechanical workshops where welding is performed and insufficient grounding may create excess currents in electronic parts. Another example is the ignition of heavy vehicle engines by large supply sources through insufficient contacts. These are primary root causes of EOS damage and the root cause can be identified and removed when this level of insight is available.

The three analysis steps can be summarized as:

- What has happened?
    - Describe the situation at which the fail occurred and which part has failed.
    - Complete failure analysis (Chapter 6) to identify the EIPD and determine possible causes.
- How has it happened?
    - Analyze the path of the stress pulse and its electrical parameters like pulse length, polarity, etc.
    - Look to replicate the EOS event at either the supplier or customer site to better understand the EIPD.
- Why has it happened?
    - Get an understanding of how the stress aggressor, victim and protection have interacted during the stress.

Examples of case studies following this pattern will be discussed in Chapter 5. Obviously, a meaningful analysis result can only be achieved if there is good supplier-customer communication in place. Getting into the specific details of the interaction of various system components leading to a fail requires in-depth insight into the system and the conditions under which the fail was observed. Insufficient information, intentionally (due to confidentiality) or unintentionally (due to limited focus), is the major obstacle for a fast and efficient analysis of EOS related problems.

The simplistic conclusion that the damaged part as victim (such as an IC) is the actual root cause of system fail and, therefore, has to be designed differently or equipped with more robustness, is usually a misconception. In general, the most time/cost efficient and fastest solution to the problem is the removal of the primary stress source (such as a faulty power supply).

4.5.1 Limitations of Analysis Methods

The expectation that any EOS event leading to damage can be detected and analyzed in this way is obviously optimistic. An essential precondition is that there is a significant failure rate which allows some statistical insight and the ability to perform tests where changes in the failure statistics can be observed. While physical failure analysis and reproduction of a failure signature by appropriate stress pulses can be performed even for a single field return, tracing back in the field is nearly impossible for fails occurring with very low repeatability. In this case, a theoretical assessment of system behavior alone can help to formulate an assumption about the root cause, but it cannot be proven. This is especially true in a situation in which a fail has only occurred once in the life time of the product. In some cases these once in a lifetime events may be due to highly unlikely ‘black swan’ events [5]. To protect system and electronic components against these events is typically very costly and only justified for highly critical systems with severe impacts as a result of any failure.

References

[1] J. Wu, P. Juliano, and E. Rosenbaum; 'Breakdown and Latent Damage of Ultra-Thin Gate Oxides under ESD Stress Conditions', Electrical Overstress/Electrostatic Discharge Symposium Proceedings 2000, pp. 287 – 295

[2] Industry Council on ESD Target Levels JEP155 (2007a) White Paper 1: A Case for Lowering Component Level HBM/MM ESD Specifications and Requirements, August 2007, www.esda.org or JEDEC publication JEP155, www.jedec.org

[3] Industry Council on ESD Target Levels JEP157. (2010a) White Paper 2: A Case for Lowering Component Level CDM ESD Specifications and Requirements, Revision 2, April 2010, www.esda.org or JEDEC publication JEP157, www.jedec.org

[4] ANSI/ESD S20.20; 2014; Development of an Electrostatic Discharge Control Program for: Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices), www.esda.org or IEC 61340-5-1; 2014; Development of an Electrostatic Discharge Control Program for: Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)

[5] Charvaka Duvvury, Harald Gossner; "System Level ESD Co-Design", John Wiley, Chichester, UK, 2015.

Chapter 5: Case Studies on EOS

Theo Smedes, NXP Semiconductors
Reinhold Gärtner, Infineon
Leo G. Henry, TLP Consultants
Hans Kunz, Texas Instruments
Alan Righter, Analog Devices
Christoph Thienel, Bosch

5.0 Introduction

This chapter describes a set of in depth case studies with failures exhibiting EOS damage. Several have been published and can be found in literature via the references.

The aim of the chapter is to provide, by using real examples, an insight into the nature of EOS problems, different ways to analyze these problems and finally to review possible solutions. Each study can be read independently of the rest. The chapter will use the same categories as used throughout the white paper and each case study is classified within the categories described in Chapters 2 and 4.

The cases will demonstrate that the initial failure analysis picture typically does not reveal the root cause. This is an example of the confusion caused by classical FA denominations as ESD, EOS or ESD/EOS. Physical analysis is an important step in the analysis, but not an adequate tool to conclude on a root cause. It will become clear that each case requires its own approach to addressing a solution and in most cases requires close cooperation between supplier and customer. These solutions are typically application specific.

The chapter will end with a summary of lessons learned and conclusions.

Description and classification of the case studies.

This chapter contains 11 individual case studies. This section briefly introduces them and classifies them according to the categories of Chapter 2 and 4.

1. Incorrect ESD qualification leading to EOS [1]
   An apparent ESD failure was actually caused by curve tracing outside AMR.
2. EOS due to misapplication [1]
   Damage after ‘loss-of-ground’ test was caused by not following application guidelines.
3. EOS due to Hot plugging [2]
   A particular manufacturing sequence caused incorrect biasing.
4. EOS due to intermittent battery ground connection
   A bad contact led to a latch-up (LU) situation which in turn caused EOS damage.
5. EOS due to ground offset
   An open in the wiring harness caused LU which led to EOS damage.
6. Knock Sensor: Harness and AMR
   Charge accumulated on the wiring harness during manufacturing may cause discharges far beyond the design limit.

7. EMI: Transient Surge
   Fast transients on the supply causes damage in extremely ESD robust transistor.
8. EMI: Board Design
   A missing resistor between VDD and GND created a potential risk for EOS damage
9. Supply capacitor switching [3]
   Slow charging of capacitor and sudden discharge caused failures during testing.
10. Manufacturing fails on a digital signal processor (DSP) [4]
    Charging of boards caused failures during assembly.
11. Reliability Testing [5]
    Burn-in testing led to EOS damage.

In Chapters 2 and 4, categories of EOS problems and ways to analyze these were introduced. The cases presented in this chapter fall into these categories as illustrated in the matrix of Table 4. The rows relate to the main branches of the EOS fishbone diagram.

Table 4: Classification of the Case Studies in the Categories of Chapters 2 and 4

	What?	How?	Why?	
	Failure Analysis	Replication of damage by controlled method	Observation in Real World	Correlation with other events
Powered Handling	1, 2, 3, 4, 5, 9, 11	1, 2, 3, 4, 5, 11	1, 2, 9	3, 4, 5, 9
Unpowered Handling	6, 10	6, 10	6, 10	
Switching/ AC operation	7, 8	7, 8		

All categories of EOS problems are addressed. The columns relate to the most essential analysis steps for each case. Ideally, the damaging event is directly observed in the real assembly or application. However, this is often not possible. In several cases, it was possible to indirectly observe the event by correlation with changes in certain process steps. A commonly used approach is to try and replicate the failure signature (electrically and physically) by means of controlled stress methods. These can include standard ESD tests, standard electromagnetic compatibility (EMC) stress tests, standard automotive stress tests, LU stress, and several forms of TLP. Obviously, this has the advantage that it can be done on individual components (IC level) or modules (PCB level) instead of on the full system, which can be as large as a car. Finally, it is sometimes possible to correlate the occurrence of failures with other events, such as changes in assembly procedures. Through the course of collecting these case studies, it became clear that ‘Replication’ is the most often used and successful analysis method. Most likely this is due to the fact that it can be done without disrupting actual manufacturing flow and to a certain extent can be completed independently by the supplier and customer.

5.1 Case 1: Incorrect ESD Qualification Leading to EOS.

Failure occurrence

A product that had been on the market for a long time was designed-in by a new customer. The customer wanted to qualify the product before starting to use it. The customer outsourced the ESD qualification to an ESD lab. The customer and ESD lab found that parts failed 2 kV HBM. The failure was determined by curve tracing on the ESD tester. The datasheet of the product quoted 3.5 kV HBM. Damaged devices were returned to the supplier for analysis.

Failure Signature

The electrical failure signature was a short of several IO pins to GND as illustrated in Figure 29.

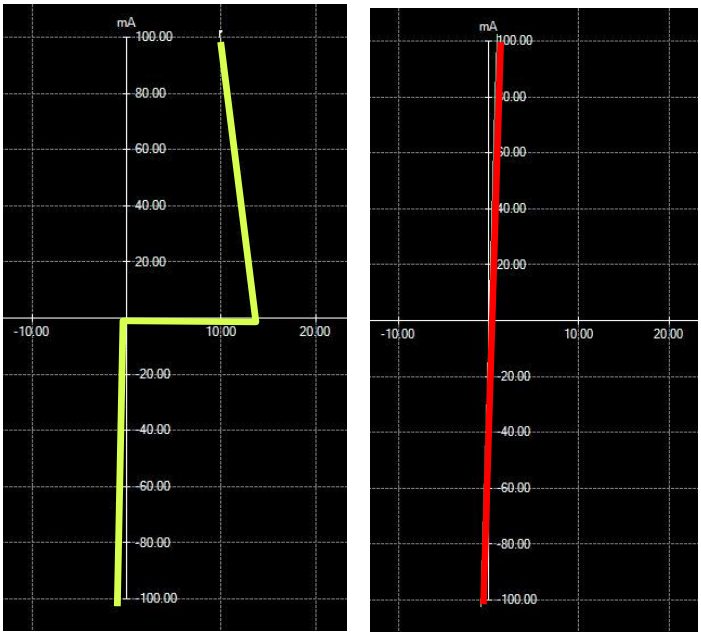


Figure 29: Curve Trace of Good Device (left) and Damaged Device (right)

Failure Location

Physical analysis revealed a damaged metal trace (EIPD location) leading to the ESD protection, as depicted in Figure 30, which strengthened the customer's opinion that the device had an ESD weakness.

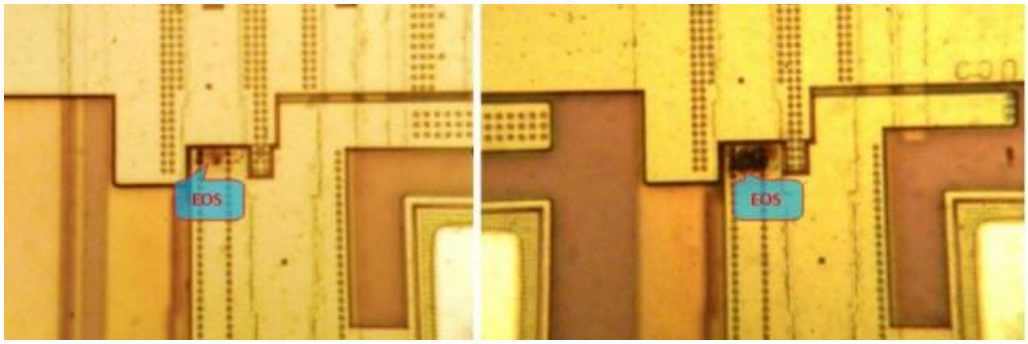


Figure 30: Optical Photo of Damaged Devices

Testing Environment

The original ESD qualification was done by the supplier with a different ESD tester than the one used by the ESD lab. By comparing software and hardware versions and knowing that a snapback-based ggNMOST protection scheme was used, it was assumed that tester artifacts were an unlikely cause of the difference in results. The customer suggested that the supplier should re-qualify the device using the same tester as the ESD lab to prove this assumption.

Root Cause

By analyzing the settings used in the test program of the ESD lab it was observed that the curve tracing was done by sweeping the voltage from -3 V to +50 V with a compliance of 100 mA. The device was specified to have an AMR of -0.5 V for negative voltages and +6.5 V for positive voltages. Also the max currents were specified to be 10 mA in both directions. The ESD protection had a trigger voltage of ~15 V. In Figure 29 it can be seen that curve tracing triggers the protection. Therefore it was confirmed that the root cause of the damage was caused by the curve tracing and not by the 2 kV ESD stress.

It was decided to send devices to an independent lab for complete HBM testing with curve trace settings in accordance to the AMR specifications. None of the devices failed up to 3.5 kV. This confirmed the originally established ESD robustness.

Analysis

For better understanding, the failure current of a pin was measured as a function of pulse duration (see Figure 31). The data shows that the failure current is less than 100 mA for pulses longer than ~10 ms. The curve tracing on the ESD tester definitely used pulses in this time range. Thus it is possible that the DC curve trace damaged the devices.

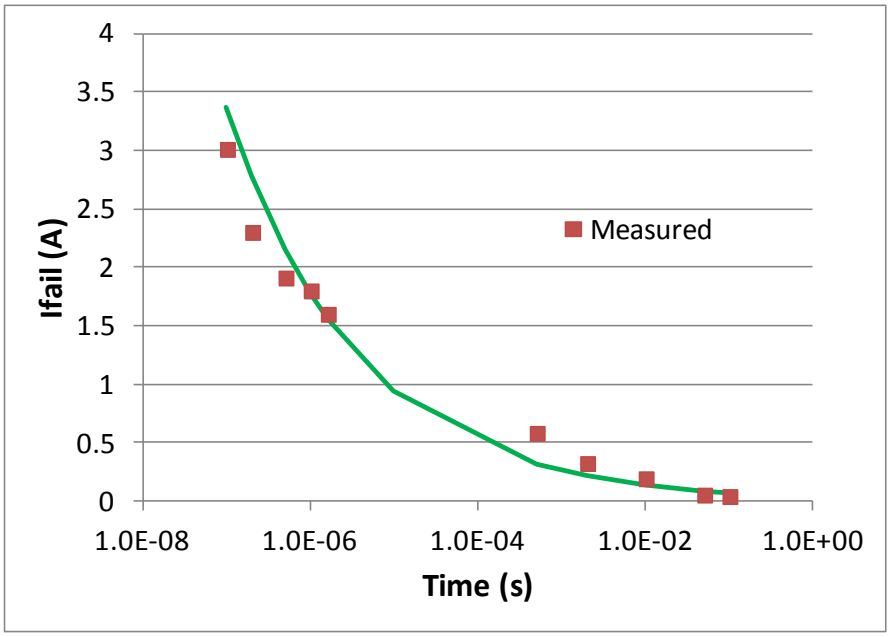


Figure 31: Power Profile

Finally, it was verified that manual curve tracing above the AMR with a 100 mA current compliance damaged fresh devices, with the same electrical failure signature.

Solution

It is not clear why the ESD lab hired by the customer performed the curve trace as described above but the solution was straightforward. After explaining the effect of driving the product outside its AMR, the ESD results obtained with the correct curve trace settings were accepted. No redesign of the product or application was required.

5.2 Case 2: EOS Due to Misapplication

Failure occurrence

A local interconnect network (LIN) transceiver which had been on the market for a long time, without showing any problems, was used by a new customer to replace a device in an existing application. The customer reported fails during 'loss-of-ground' application testing. The application stopped functioning. They commented that the product was robust for ISO-7637- Pulse 2a stress-test, hot switching or a short circuit test.

Failure and Location

After physical analysis it was observed that the fails were related to the EIPD location as shown in Figure 32. A metal trace was damaged, leading to a short between the supply and a bus. This failure mode was not observed during the IC qualification or through other customer returns.

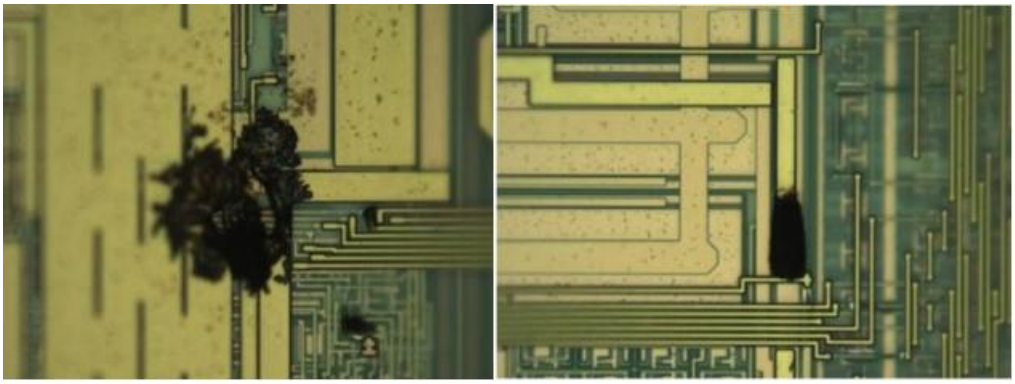


Figure 32: Optical Photo of Damaged Devices, Two Locations on the Same Track

Analysis

The device was characterized by TLP. For positive pulses, all pins were damaged at extreme voltages, which were unlikely to occur in the application. For negative pulses, the lowest failure levels were observed for the battery pin. Further characterization showed that the failure point decreased quite rapidly with increasing pulse duration, as illustrated in Figure 33. The circuit associated with the damage location basically consists of a single, relatively high ohmic diode, in parallel with 3 diodes in series. This explains the change of slope when the voltage gets below -3 V. The damage is in the single diode track. By separating the currents over these 2 branches the current required to damage the diode track can be extrapolated and subsequently the voltage required for damage can be plotted vs. pulse duration. The result is shown in Figure 34. From this it can be concluded that damage is possible at relatively small voltages if they are applied for sufficient amount of time. For example, at -3 V (the kink point), the expected life time is just a few tens of microseconds.

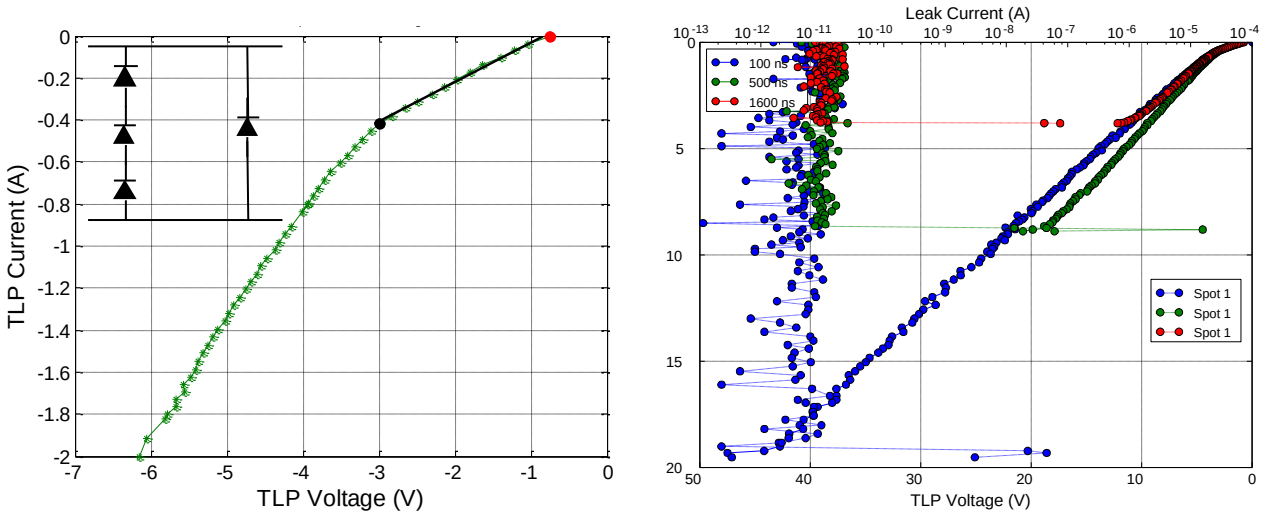


Figure 33: TLP Characteristics of Pin Associated With the Damage.
Note the significant reduction in the TLP fail voltage and current at pulse widths of 500 ns and 1600 ns as compared to the 100 ns pulse width.

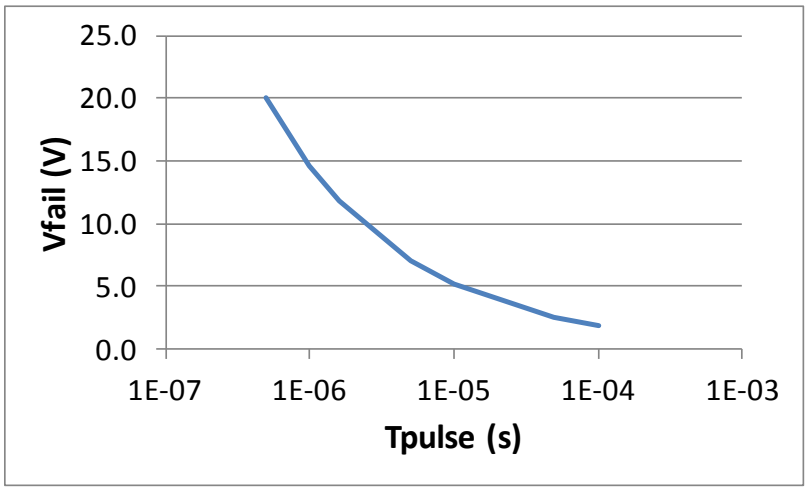


Figure 34: Calculated Failure Voltage Profile

Root Cause

Figure 35 shows a simplified sketch of the application. When the switch S1 is closed the capacitor C1 needs to be charged. In a loss of ground situation for module 1 this causes a severe ground bounce. The test was done because the customer expected that a loss of ground could happen during the life time of the design. For example, this could happen during service or maintenance of the car, where this module would need to be temporarily removed or replaced. This is equivalent to a negative pulse on the supply of the IC. In-situ measurements during the test showed -6 V on the IC supply for ~100 µs. As demonstrated above, this is sufficient to damage the IC. The datasheet specified an AMR of -0.5 V and the use of a series diode in the supply line to block reverse current.

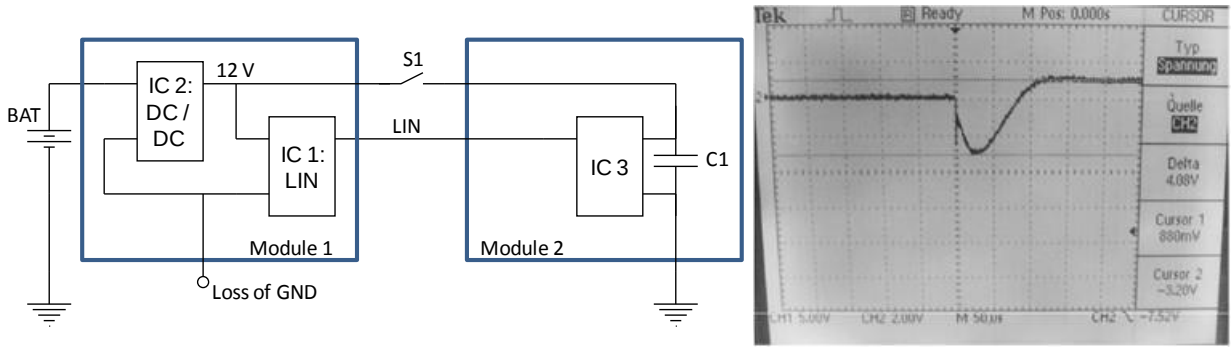


Figure 35: Simplified Schematic (left) and Signal Leading to Damage (right)

Solution

The customer decided to add the external series diode on the PCB as well as an external diode to clamp the voltage to low negative voltages for overshoots, as shown in Figure 36. After adding these diodes the ground bounce was limited to less than 0.5 V and the voltage on IC1 was limited to ~4 V with a duration of less than 1 µs. As expected, this resolved the problem. No failures were observed and the product was taken into production. As discussed above, the expectation is that a

loss of ground could be possible during the life time of the design, practically speaking this could be consider a hot plugging event. In this case, the EOS damage was not a field return, but occurred during a customer qualification test to verify that the system was robust against such occurrences in the field. Therefore, the real root cause is the deliberate loss-of-ground.

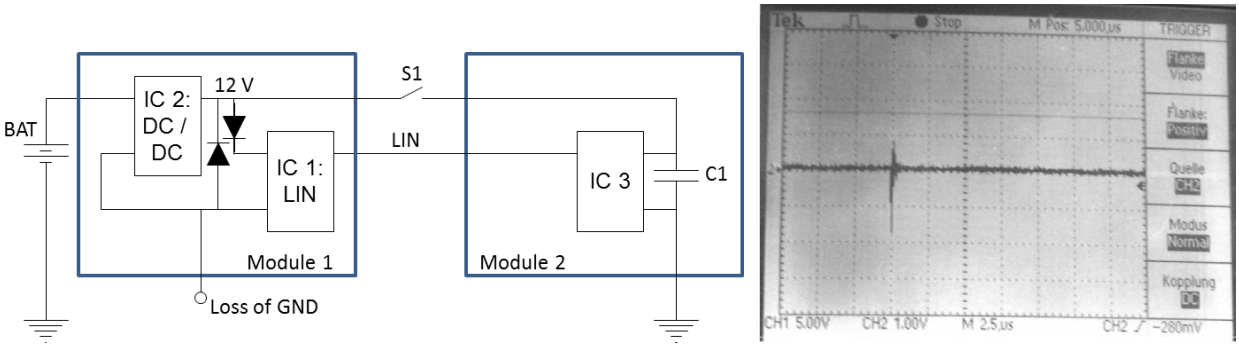


Figure 36: Simplified Schematic of Solution (left) and Resulting Signal during Stress (right)

5.3 Case 3: EOS due to Hot Plugging

Failure Occurrence

Vehicle manufacturer X produced the identical vehicle model at two different locations, A and B. Both production lines used the identical model of airbag ECU (called ECU1 in figures below). The production volumes at both lines were comparably high. From location A the vehicle manufacturer reported a large number of failed airbag ECUs. From location B however, not even a single failed airbag ECU was reported.

Failure Mode

Analysis of the failed airbag ECU revealed that in all cases, a similar EIPD location was seen on the application specific integrated circuit (ASIC) as shown in Figure 37. At the transceiver of the local interconnect network (LIN) interface, a coupling diode to the central ESD protection circuit was melted due to a suspected electrical overstress.

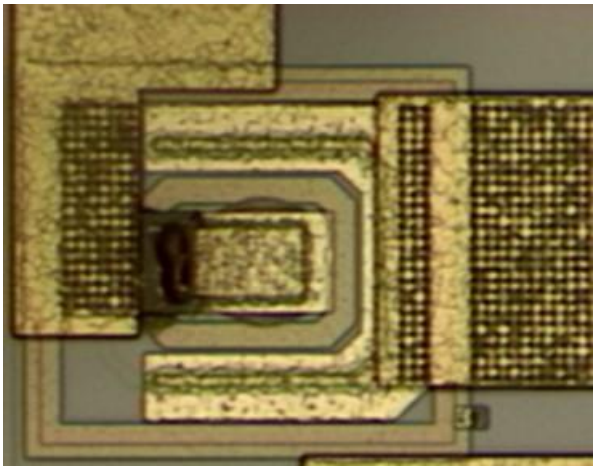


Figure 37: Optical Photo of Melted Coupling Diode (Customer Complaint)

Analysis and Simulation

In order to prove that the melted protection diode was caused by an event which resulted in EOS damage and not by a device weakness, many trials were done on the ASIC level. ASICs were stressed at the LIN bus terminal pin by positive and negative voltage pulses (charged capacitance) in order to reproduce the failure mode. The trials (see Figures 38 to 41) showed that the melting of the coupling diode could solely be reproduced by positive voltage pulses beyond the specified absolute maximum ratings which in this case had an upper limit of +36 V.

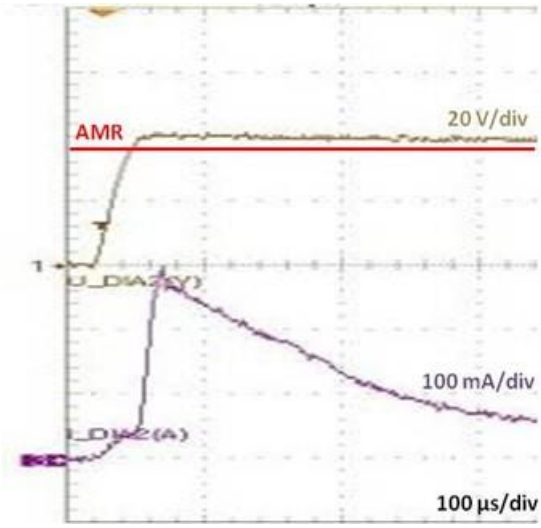


Figure 38: I/V Characteristics at LIN Bus Terminal – No Damage

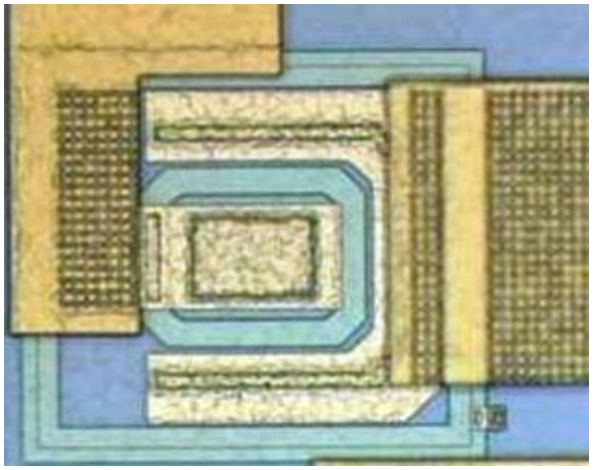


Figure 39: Optical Photo of Coupling Diode after Stress, @ C = 20 µF, U_C = 42 V – No Damage

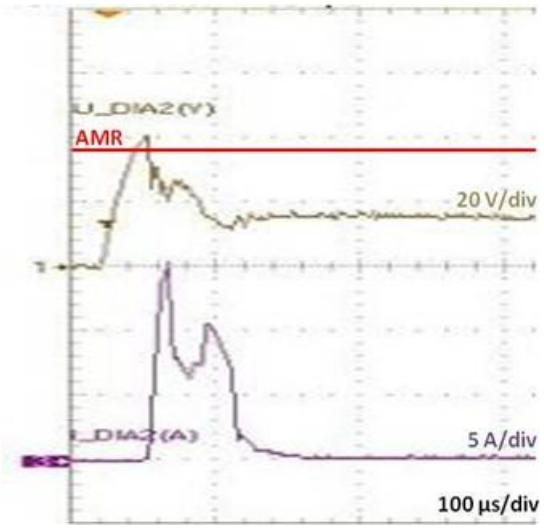


Figure 40: I/V Characteristics at LIN Bus Terminal – Creating Damage

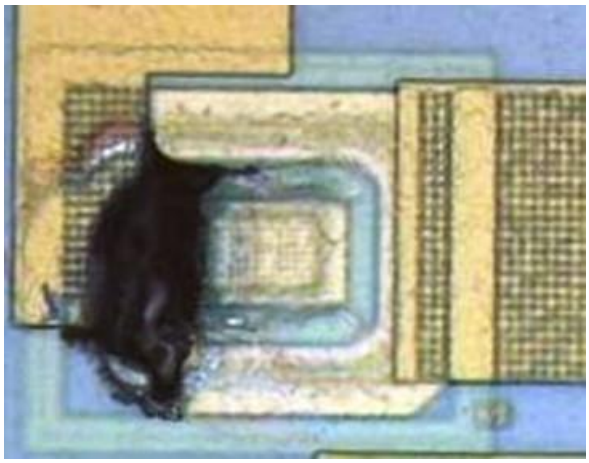


Figure 41: Optical Photo of Melted Coupling Diode after Stress @ C = 20 µF, U_C = 43 V

Investigations on the ECU and vehicle level were also made. The LIN bus terminal of the airbag ECU (ECU1) was connected to another ECU (ECU2) by several meters of long wire (see Figure 42).

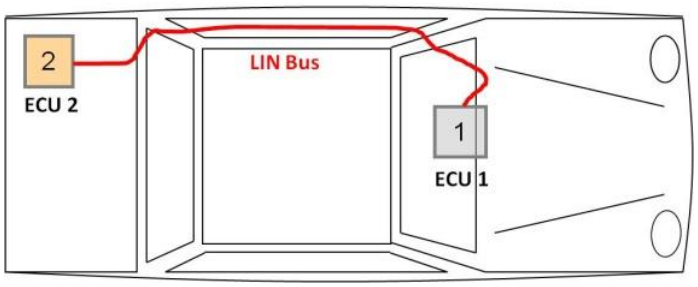


Figure 42: Sketch of ECU Mounting Locations

Trials in the lab revealed that during hot plugging of ECU2, voltage peaks significantly higher than 40 V could arise on the LIN bus terminal of ECU1. This was due to the interaction of contact bouncing, a ground contact established too late and the inductance of the LIN bus wire.

Investigations into the production processes of the vehicle manufacturer's plants A and B revealed a significant difference in the assembly process steps for ECU1 and ECU2. In both lines, ECU1 was mounted before ECU2. But in line A the assembly of ECU2 was carried out with an energized vehicle wiring system (hot plugging). In line B however, ECU2 was installed before the vehicle wiring system was energized.

Root Cause

The connecting of ECU2 to the energized vehicle wiring system (hot plugging of ECU2) caused high voltage and current peaks on the LIN bus. One reason for this was the undefined contact sequence at the ECU plug during the plugging process (see Figures 43 and 44). Depending on the angle of the wiring harness connector during the plugging process, the supply voltage pin and other ECU pins could have been electrically connected while the ground connection was still open. This resulted in undefined voltage and current peaks on the LIN bus. The long (several meters) LIN bus wire, and consequently higher inductance, additionally increased the amplitudes of the voltage pulses.

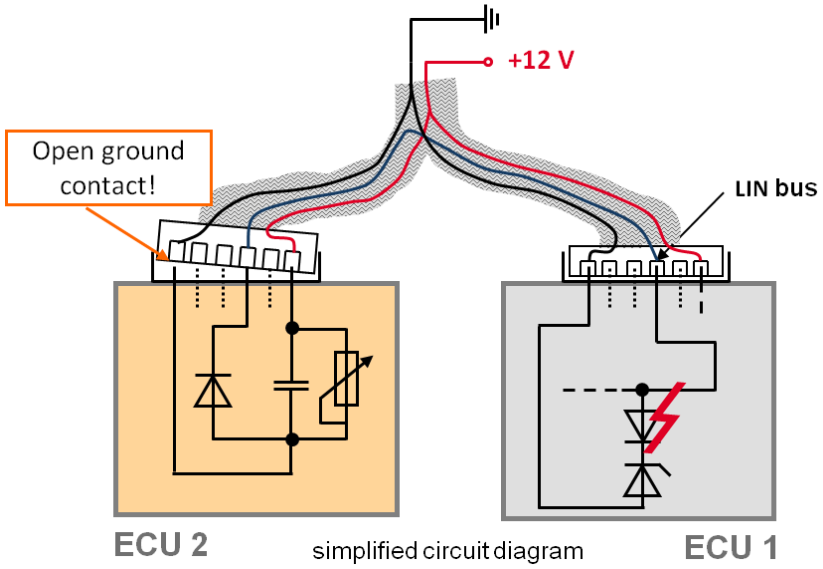


Figure 43: Hot Plugging of ECU2; Mechanical Diagram

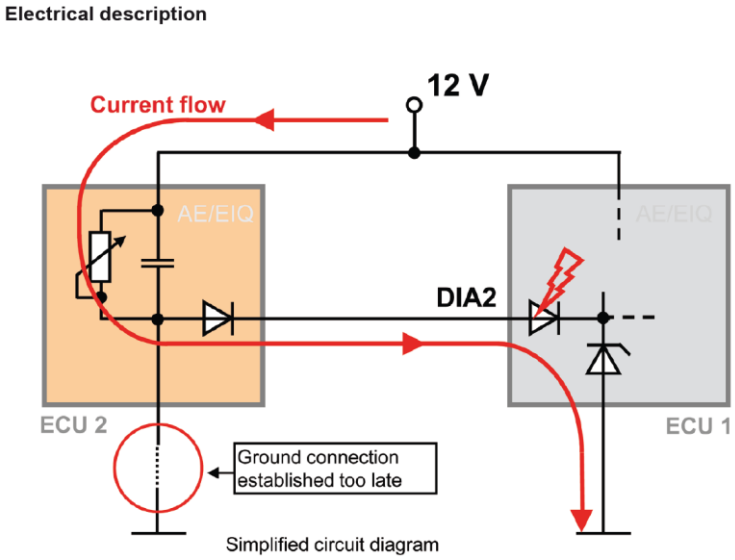


Figure 44: Hot Plugging of ECU2; Electrical Diagram

Solution

The vehicle manufacturer modified the production process at line A to be identical to that of line B, resulting in no further damage occurring on line A.

5.4 Case 4: EOS due to Intermittent Battery Ground Connection

Failure Occurrence

From time to time, a vehicle manufacturer claimed defective ECUs that failed in the production line.

Failure Mode

Physical analysis of the failed ECU revealed that in many cases an ASIC had EIPD in the same location as shown in Figure 45. A double-diffused metal-oxide-semiconductor (DMOS) transistor and some other circuits in the immediate vicinity were damaged.

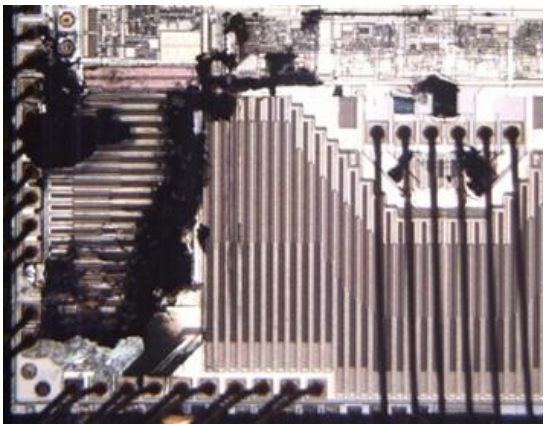


Figure 45: Optical Photo of Damaged DMOS Transistor (Customer Complaint)

Analysis and Simulation

In order to prove that the damage was caused by an EOS event and not by a device weakness, many investigations and simulations were carried out on the ECU and ASIC level. Extensive investigations with the ASIC supplier showed that a negative voltage drop on the ECU internal 5 V supply voltage U_5V which supplied the ASIC (see Figure 46) could cause a latch-up on the ASIC. The result of the latch-up was damage to the ASIC similar to the customer complaints. The negative voltage necessary to trigger the latch-up had to be clearly outside the specified AMR of the ASIC. For a long time it was not clear how a negative voltage at the ECU internal 5 V voltage supply could be generated inside an ECU installed in a vehicle.

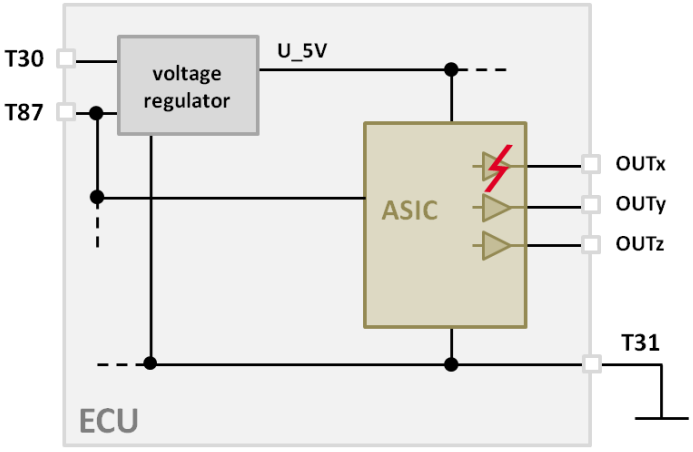


Figure 46: Simplified Circuit Diagram of ECU

The breakthrough was achieved by investigation and measurement at the vehicle level. Simulations found that contact bouncing of an incorrectly fixed ground terminal at the vehicle battery sometimes

caused negative voltage peaks on the ECU supply voltages U_T30 and U_T87 and, as a consequence of this, also on the ECU internal 5 V supply voltage U_5V (see Figure 47). But to damage the ASIC, as depicted in Figure 48, it was necessary for the ECU supply voltages U_T30, U_T87 and U_5V to all be negative concurrently with the voltage at the drain of the concerned DMOS (U_OUT) remaining above a certain level. This was found to occur within a narrow time frame of less than 2 ms.

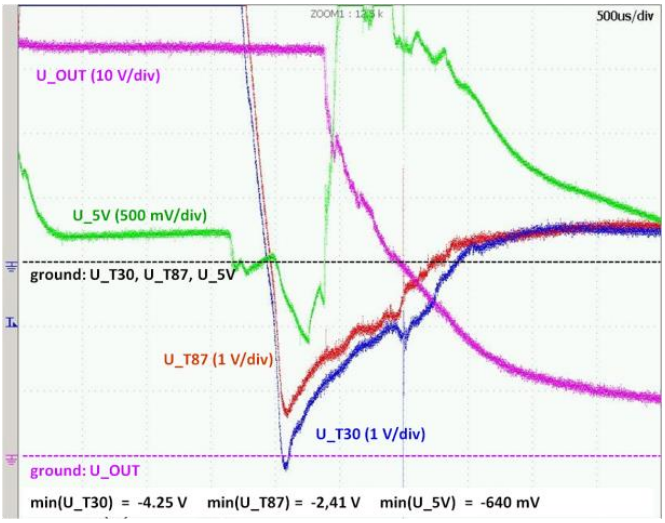


Figure 47: Critical Voltage Characteristics during Bouncing of Battery Ground Terminal

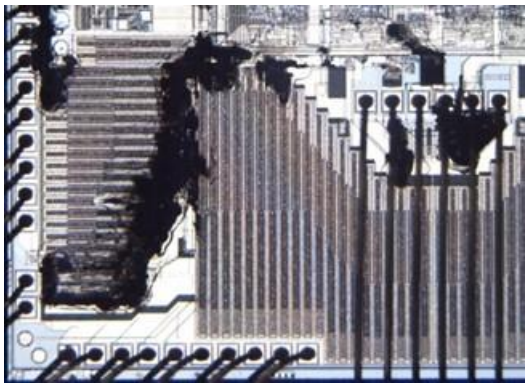


Figure 48: Optical Photo of Burnt DMOS Transistor after Bouncing of Battery Ground Terminal

Root Cause/Summary

An incorrectly fixed ground terminal at the vehicle battery caused contact bouncing. Due to this, negative voltage peaks were induced on the external and internal voltage supply lines of the ECU. These negative voltage peaks outside the specified AMR of the ASIC sometimes caused a latch-up event on the ASIC which lead to the destruction of the ASIC. Through the investigation it could be clearly demonstrated that not a device weakness but an electrical overstress event created the latch-up which caused the failures in the customer's production line.

5.5 Case 5: EOS due to Ground Offset

Failure Occurrence

Over a short period of time, a vehicle manufacturer identified several electronic control units which failed in a newly introduced vehicle model. All failing ECUs were field returns with low mileage. They were sent to the ECU supplier for analysis.

Failure Mode

The analysis of the failed ECU revealed that on all returned ECU a certain sensor evaluation ASIC was defective. Physical analysis of the ASIC by the semiconductor manufacturer revealed an EIPD location that in all cases was a metal track in the ASIC's internal 5 V voltage supply as shown in Figure 49.

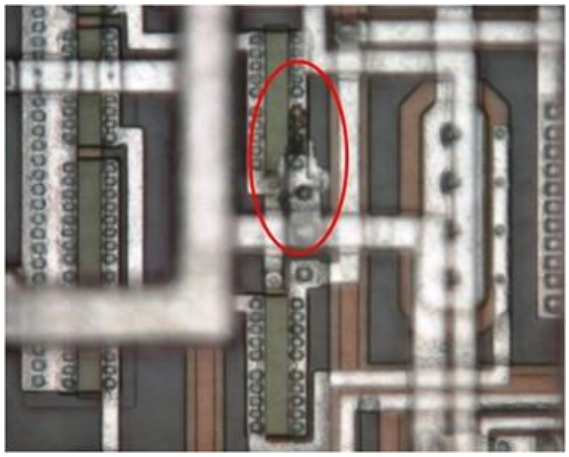


Figure 49: Optical Photo of Damaged Metal Track (Customer Complaint)

Theoretical considerations and trials in the lab at the ASIC level showed that negative voltage pulses far beyond the specified AMR on the sensor signal inputs of the ASIC could cause a latch-up event which, depending on its characteristics, could result in a damaged metal track consistent with the customer complaints.

Based on these results, investigation measurements and trials on two vehicles of the same automotive line were carried out in order to find out whether negative voltage peaks could occur during normal vehicle operation. The investigations revealed that the operation of the ignition coils induced a ground offset between engine ground and chassis ground of the vehicle. The maximum value measured for the ground offset was seen to be -8.4 V (see Figure 50).

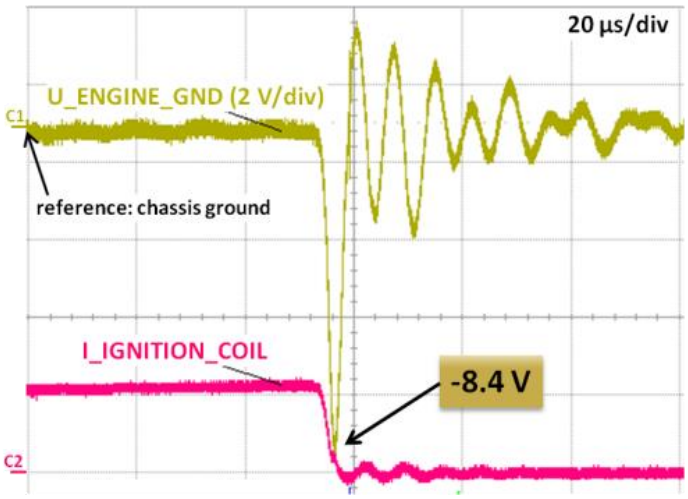


Figure 50: Ground Offset Caused by Switching Off the Current at the Primary Side of an Ignition Coil

The ground reference of the ECU was chassis ground. Engine and chassis were electrically connected by a ground strap. The sensor which was evaluated by the concerned ASIC was mounted on the engine block (see Figure 51). Under normal operation, the sensor had no electrical connection to engine ground.

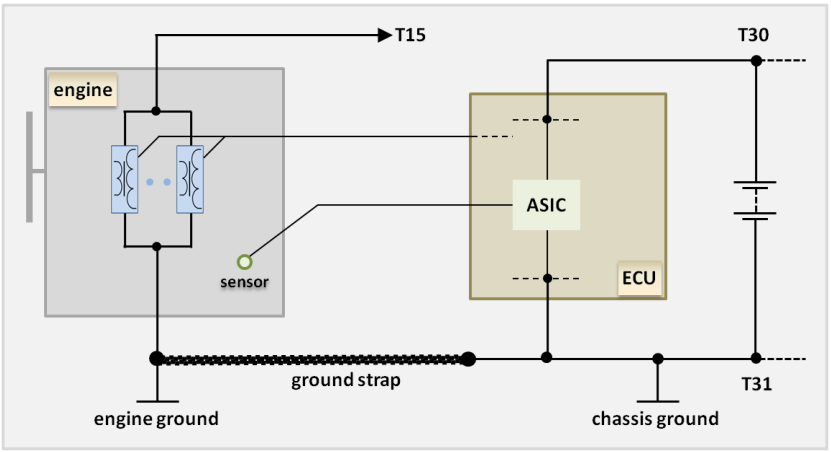


Figure 51: Schematic of Ground Wiring

By means of trials carried out at the vehicle level, it could be demonstrated that a short-circuit of a damaged sensor wire (damaged insulation) to engine ground in conjunction with the ground offset described above could trigger a latch-up event inside the ASIC. The latch-up state could be monitored through increased current consumption of the ASIC. In most cases, the latch-up did not lead to damage of the ASIC but to a malfunction of the ASIC and ECU. After switching the ECU off and on the operation of the ECU and ASIC were in accordance to specifications again. But if the ASIC was damaged by latch-up, the failure mode was identical to those of the customer complaints (see Figure 52).

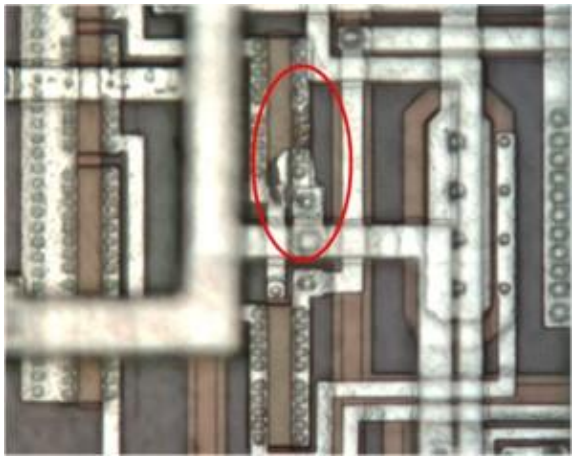


Figure 52: Optical Photo of Damaged Metal Track after Trials on Vehicle Level

Root Cause

The operation of the ignition coils caused a pulsed ground offset between the chassis ground and the engine ground of the vehicle. From the ASIC's point of view the voltage level of this ground offset was negative. The ground offset of the engine block in conjunction with a short circuit of a damaged sensor wire to this engine block could cause a latch-up at the ASIC which in turn could lead to damage of the ASIC. The negative voltage levels which could be measured at the sensor inputs were far beyond the specified AMR of the ASIC. So latch-up, which resulted in electrical overstress, was the cause of the damage to the ASIC and ECU. Short circuiting of the engine block wire was the root cause.

Solution

On inquiry, the vehicle manufacturer reported that at the time the ECU damage occurred, there was also a problem with the wiring harness of the ECU. Therefore, the wiring harness was modified. Since then no further ECU damage has occurred.

5.6 Case 6: EOS Case Study "Automotive Knock Sensor"

This case study is based on a root cause diagnosis that was conducted in collaboration with a semiconductor manufacturer and a Tier 1 automotive supplier.

Failure Occurrence

Throughout a 4 year period, an automotive OEM reported multiple 0 km failures of an ECU. All of these failures occurred in the winter period in one of the OEM's engine plants located in Europe, and only when the relative humidity of the air dropped below 20 %. A sketch of the application is shown in Figure 53. The ESD robustness of the ECU is 8 kV according to ISO 10605 (discharge into the open off-board connector pins). The ESD robustness of the ECU is more than sufficient for the manufacturing floor of the engine plant. In an audit of the manufacturing floor of the engine plant no obvious problems were found.

The failing ECUs were returned to the responsible Tier 1 for failure analysis. The Tier 1 narrowed the failure down to the knock sensor input pin of an IC, highlighted in red in Figure 53. The failing ICs were returned by the Tier 1 to the IC manufacturer for failure analysis.

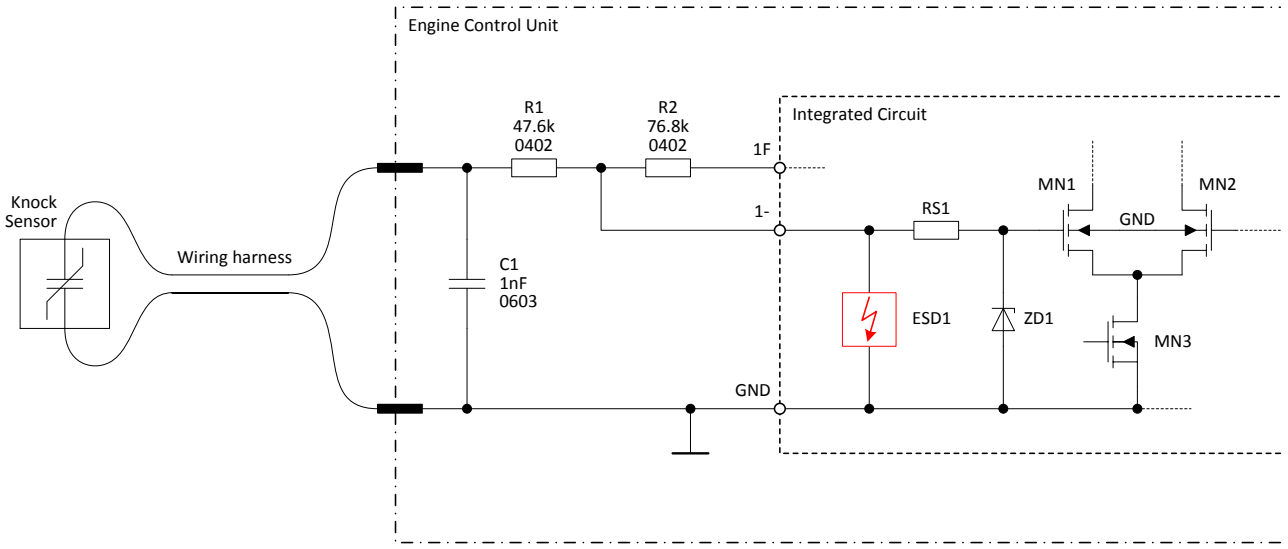


Figure 53: Simplified schematic of the knock sensor application. The damaged ESD protection element ESD1 in the IC is indicated in red.

In the subsequent failure analysis, the IC manufacturer found that the EIPD location in all failing ICs was the ESD protection element, ESD1, connected between pin "1-" and pin "GND". The FA result and a cross-section of the ESD element are shown in Figures 54 and 55, respectively.

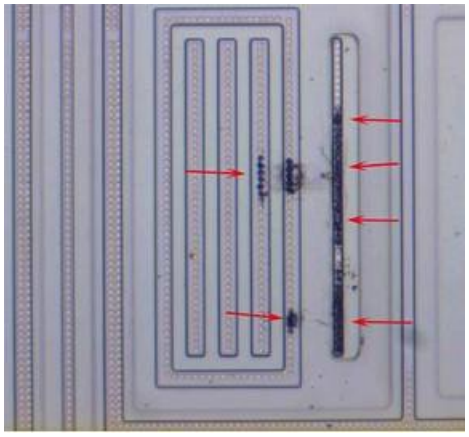


Figure 54: Damaged ESD protection element ESD1 deprocessed down to Silicon

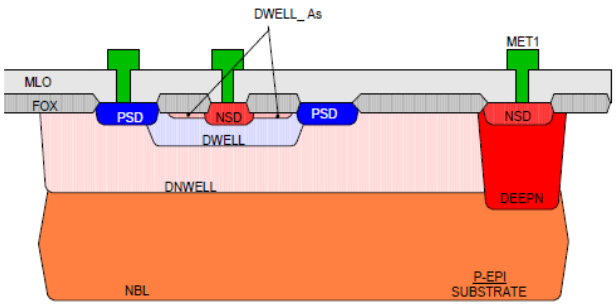


Figure 55: Cross-section showing the construction of the damaged ESD protection NPN transistor ESD1

The damage suggests an energy driven failure mode. The ESD robustness of the ESD transistor ESD1 and the entire IC is excellent. The ESD transistor ESD1 is proven and reliable. A summary of the device data are shown in Table 5.

Table 5: Device Data Summary

ESD Protection Element ESD1	Type = negative-positive-negative (NPN) transistor Breakdown Voltage ≅ +22 V / -0.7 V Clamping Voltage ≅ +30 V / -3…-5 V
Abs. Max. Ratings of Pin "1-" w.r.t. GND	+14 Vdc / -0.3 Vdc
ESD Robustness	4 kV HBM (E_{diss} ≅ 12 µJ) 1.5 kV CDM (E_{diss} ≅ 5.8 µJ)
LU Robustness	100 mA (P_{diss} ≅ 2.7 W)

The ESD and latch-up (LU) qualification results of the IC (indicated by marker symbols) match quite well with the estimated power-to-failure of the ESD transistor ESD1 (solid line) as shown in Figure 56.

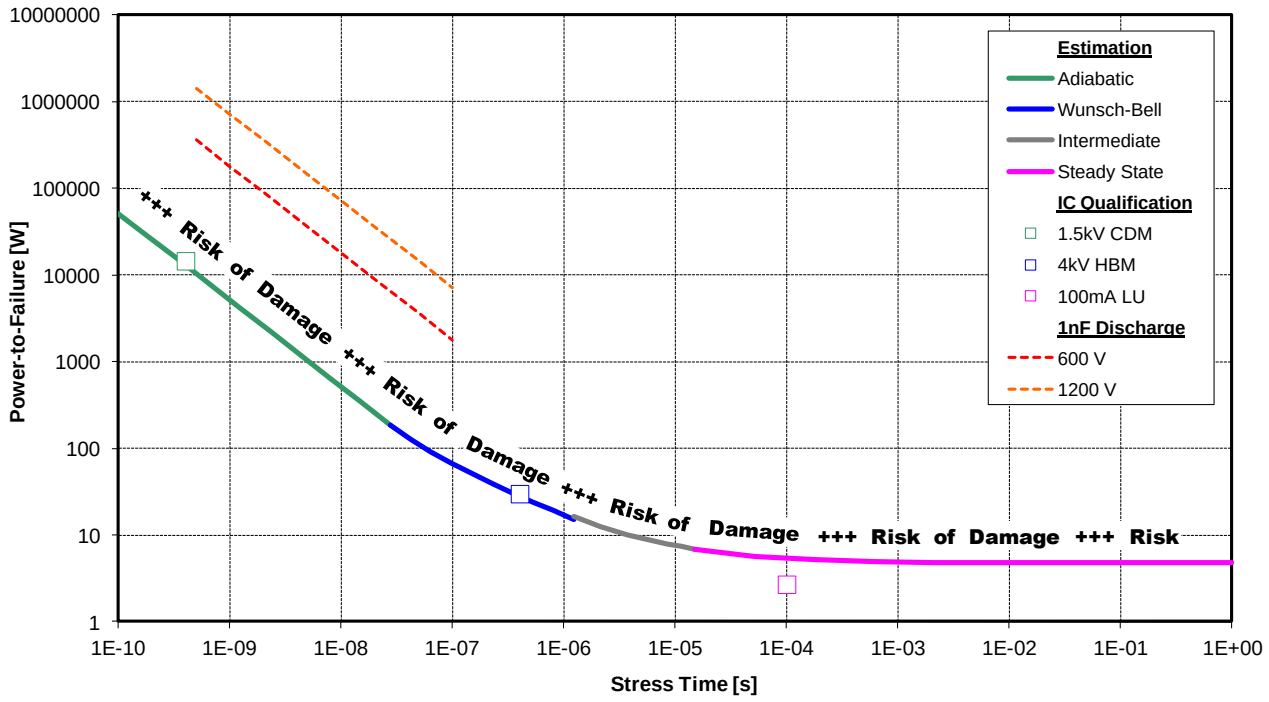


Figure 56: Power-to-failure data of the damaged ESD transistor ESD1: Estimated power-to-failure characteristic (solid line), dissipated powers at 1.5 kV CDM, 4 kV HBM and 100mA LU (marker symbols) and dissipated powers of a 600 V and 1200 V discharge of a 1nF capacitor into the ESD transistor (dashed lines).

The damaged IC pin "1-" is connected via resistor R1 and capacitor C1 to off-board connectors of the ECU, which are connected via a wiring harness to a knock sensor.

The characteristics and sensitivities of the knock sensor suggested that it may have been charged up during the manufacturing process in the engine plant and may have discharged uncontrolled into the ECU and into the IC. Experiments with charged knock sensors that were directly discharged into the ECU supported this hypothesis, since they showed the same failure signature of the IC as the actual 0 km failures.

Assuming that a 1 nF capacitor, charged up to a voltage between 600 V and 1200 V, discharges directly via pin "1-" into the ESD transistor ESD1, a dissipated power as indicated by the area between the red and orange dashed lines is expected as shown above in Figure 56.

This leads to the following questions:

How does C1 become charged?
How is charge delivered to “Pin 1-” without R1 acting to limit current?

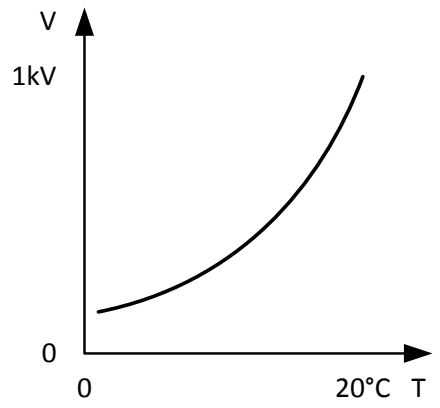


Figure 57: Typical temperature dependency of the knock sensor's output voltage

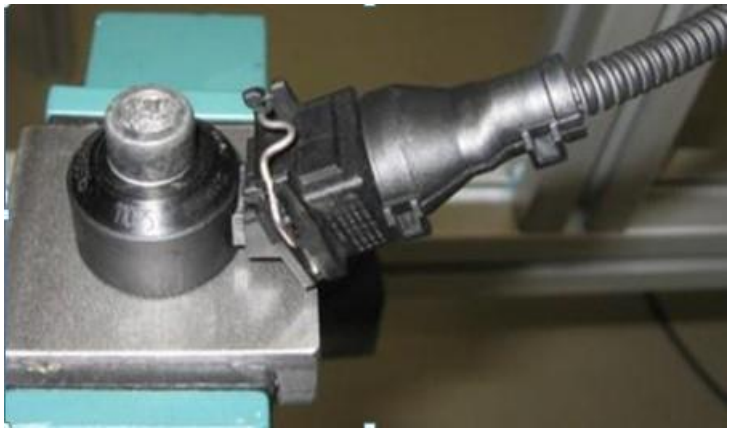


Figure 58: Photo of the knock sensor (on the left) and its connection to the wiring harness

Failure Mechanism

1) When the knock sensor is fastened to the engine or is subjected to temperature changes in the engine plant, it was found to charge up to voltages in the range of 1000 V to 1500 V as shown in Figure 57.
2) As the charged knock sensor was then connected to the wiring harness, it charged the wiring harness (see Figure 58 for the connection).
3) After the ~1.5 hour assembly of the engine is completed, the ECU is connected to the wiring harness. The humidity of the air in the engine plant is not controlled. If the relative humidity exceeds 20%, the knock sensor and the wiring harness can discharge before the ECU is connected to the wiring harness.
4) If the relative humidity of the air is less than 20%, the knock sensor and the wiring harness may still be charged up to ~1200 V when the ECU is connected to the wiring harness. This condition

is reached during cold winter months. As the ECU is connected to the wiring harness, the residual charge of the knock sensor and the wiring harness discharge into the ECU (cable discharge event, see Figure 59).

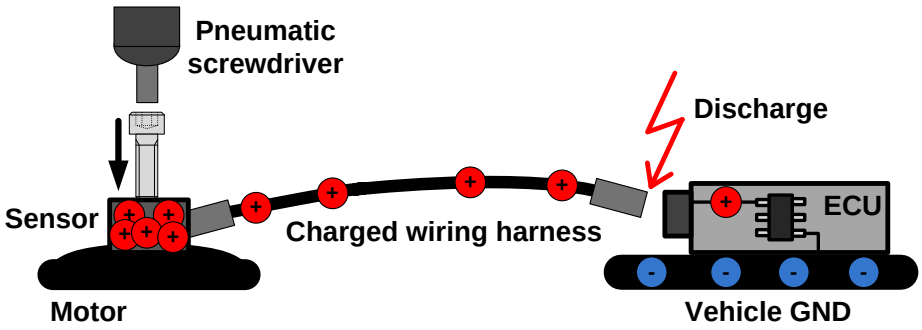


Figure 59: Discharge of the charged knock sensor and wiring harness into the ECU and its IC.

5) At voltages below 2000 V the sparking distance of air discharges is short and discharges occur very rapidly (within 100 ps). In this time domain, the decoupling capacitor C1 shown in Figure 53 is ineffective due to its parasitic series inductance. As a result, the charging voltage of the knock sensor and the wiring harness is directly applied to the series connection of the resistor R1 and the ESD transistor ESD1 in the IC. Thus, C1 could be interpreted as the root cause, but C1 is only the cause of the problem. The root cause is the uncontrolled charging and discharging of the knock sensor and the wiring harness before they are connected to the ECU.

6) Since the ESD transistor ESD1 is designed to clamp voltages to ~30 V, almost the complete charging voltage is forced to drop across the surface mount device (SMD), resistor R1.

7) The SMD, resistor R1, is a 0402 form factor. This form factor is characterized by L = 1 mm, W = 0.5 mm and D = 0.25 mm (see Figure 60). The area of R1 on the PCB is 0.5 mm^2. This resistor is not able to isolate the high charging voltage of the knock sensor and the wiring harness. As a result, a sparkover occurs between its terminals.

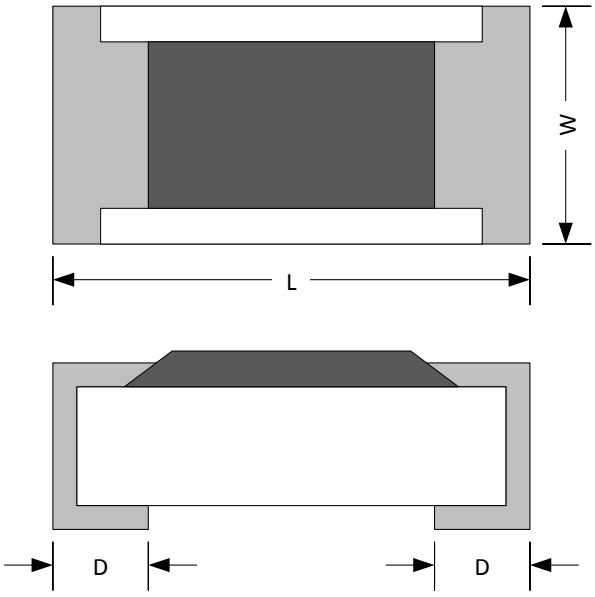


Figure 60: Top view and side view of the 0402 SMD resistor R1.

8) Due to this sparkover, almost the complete energy stored in the charged knock sensor and the wiring harness discharges into the ESD transistor ESD1 of the IC. The power that is dissipated in the ESD transistor falls into the range between the red and orange dashed lines in Figure 56. Hence it exceeds the power-to-failure of the ESD transistor and results in EOS damage to the ESD transistor. From the analysis above, it is clear that the actual root cause for this EOS damage was an uncontrolled discharge of the knock sensor and the wiring harness before they were connected to the ECU. A contributing factor was the insufficient voltage rating (form factor) of the SMD resistor.

Solution

After completion of the analysis that was conducted in cooperation with the Tier1 supplier, no additional returns occurred. The supplier did not give details on what exactly was done to remove the problem.

5.7 Case 7: EMI – Transient Surge

Failure Occurrence

One customer returned several devices with a unique failure signature. All returns were from a new application and most of them came from the OEM production line (0 km). The same device had been running in other applications and with other customers without any problem.

Failure Mode

Physical failure analysis found a liquid crystal thermography (LCT) spot at the corner of the ESD protection of the failing status pin (see Figure 61) and further SEM work found the EIPD location as shown in Figure 62, indicating pin leakage to ground and physical silicon damage.

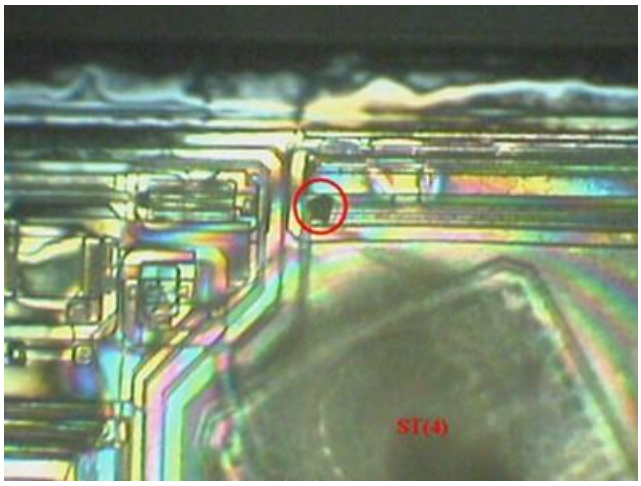


Figure 61: LCT Spot View in the Corner of ESD Diode.

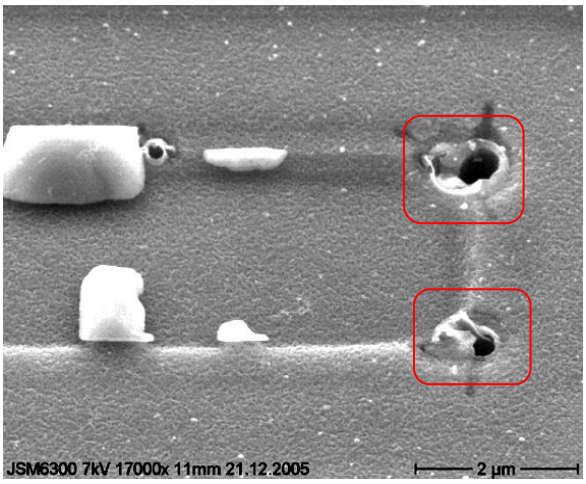


Figure 62: SEM Picture after Delayering.

Analysis and Simulation

Such tiny punch holes are an indicator for fast voltage transient failures, typically caused by ESD. But since the device has an ESD robustness > 25 kV, fast transients in the system are more likely the root cause as opposed to ESD.

The ESD device of the affected STATUS (ST) pin has a parasitic NPN transistor between its cathode and substrate (Vbb) with base on ground as shown in Figure 63. Therefore, the ESD device can be overstressed by a stress voltage applied between the pin and ground or by a stress voltage applied between substrate and ground with the affected pin having a low ohmic path to ground.

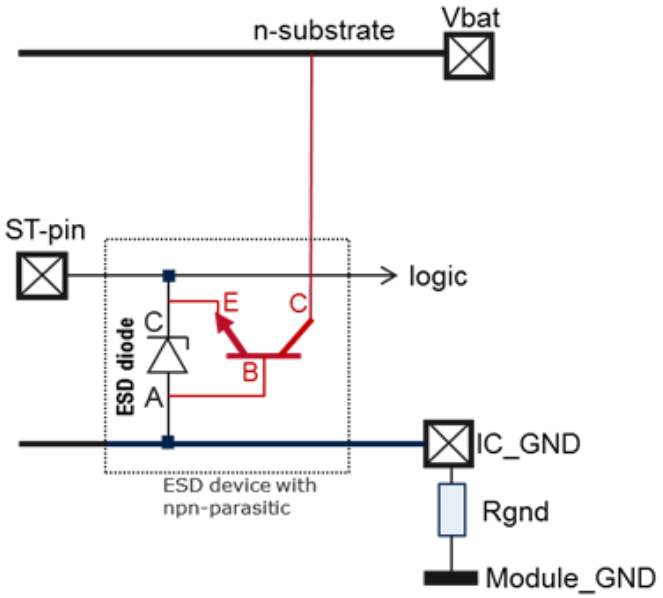


Figure 63: Parasitic NPN Connection off of the ESD Diode

In the customer's application, the affected pin was connected to ground with a 10 nF capacitor, which provides a low-ohmic connection to ground only for fast transients. Additionally, the device ground has a connection to system ground via a 150 Ω resistor. Both elements can favor the damage of the ESD diode in the case of a transient voltage at the Vbatt pin. This could also be confirmed by a stress simulation with ISO pulses (ISO-2a pulses according to ISO 7637) in a setup close to the final application (see Figure 64). The 150 Ω resistor was needed as a protection against load dump and reverse battery polarity and could therefore not be removed.

When the ISO-tests were performed with the 10 nF capacitor on the board the device failed during 75 V ISO-2a pulses which aligned with the same failure signature as the customer return. When the 10 nF capacitor was removed from the board, the low-ohmic connection (for transients) to ground was gone and the device survived 250 V ISO-2a pulses.

When the transients were suppressed by two 1000 µF capacitors in parallel with a 10 nF capacitor at Vbatt (see Figure 64), the device survived the 250 V ISO-2 pulses even with the 10 nF capacitor at the ST pin.

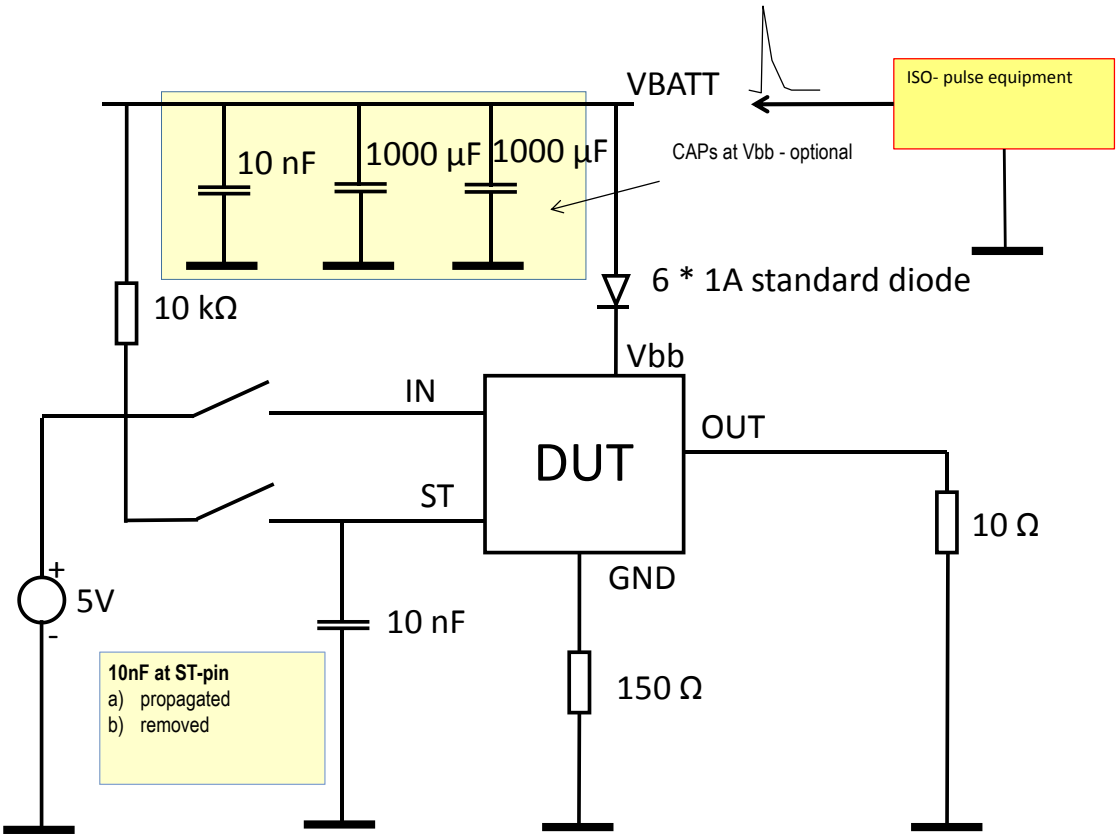


Figure 64: Schematic of Test Setup with an Application-like Board

Root Cause/Summary

The 10 nF capacitor at the affected pin was found to be a potential cause for damaging the ESD diode during a fast transient stress at Vbatt. A voltage transient (ISO-2a pulse) was used in the lab to recreate the same damage signature at the ESD diode of the affected pin as in the customer return.

The recommendation was to remove the 10 nF capacitor at the affected pin. Once the recommendation was implemented on the board, no additional damage signature was reported.

Note: the root cause of the problem (i.e. the EMI source) could not be confirmed as one specific event, but low voltage ISO-pulse like events are very common in car assemblies.

5.8 Case 8: EMI – Board Design

Failure Occurrence

Devices with a unique damage signature had been returned from one customer coming from a new application. The returns came from Tier 1 and OEM production, but also from the field (end user). The majority of damaged devices came from the Tier 1 production. This same device, running in other applications and at other customer sites, had not exhibited any problems.

Failure Mode

The electrical signature is a short between VDD and GND and a short between Vbb and GND. Physical failure analysis indicated three different EIPD signatures/locations, which can only be generated if a high current is flowing for a significant duration:

1. Burnt metal at the VDD pad: all devices showed this type of damage (Figure 65)
2. Burnt metal at the GND-DMOS: only a few devices showed this damage (Figure 66)
3. Burnt metal at the GND pad: only one device showed this damage (Figure 67)

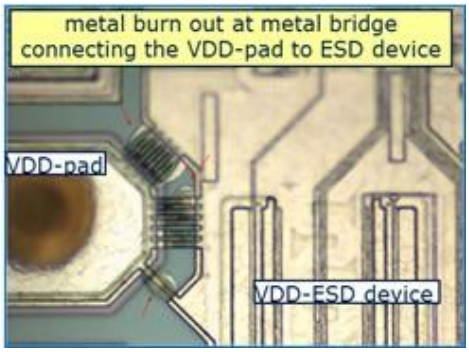


Figure 65: Burnt Metal at VDD pad

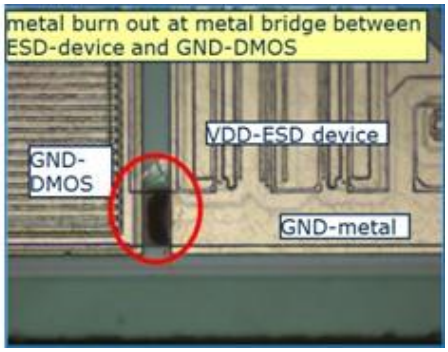


Figure 66: Burnt Metal at the GND-DMOS

Figure 67: Burnt Metal at GND-Pad

Analysis and Simulation

From the physical failure analysis it is known that a high current had to flow for a long duration to create such damage. To find out what type of stress might have caused the damage, without having more information from the customer, parametric elements of the used technology had to be considered. Figure 68 depicts a schematic representation displaying the locations of the damage shown in Figures 65-67.

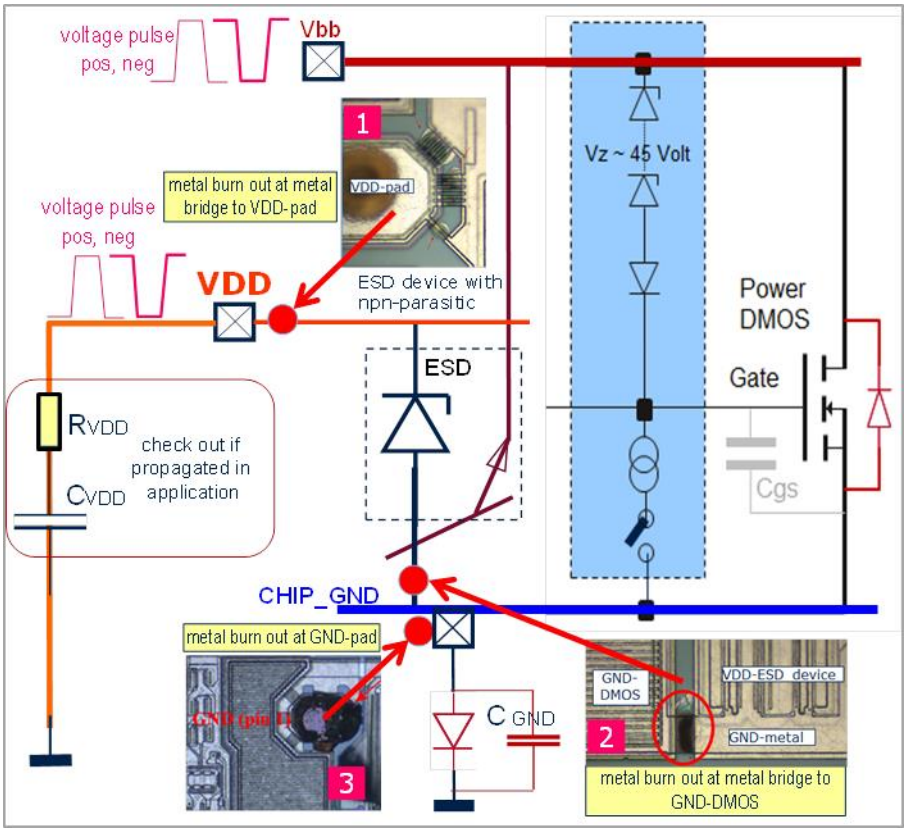


Figure 68: Schematic of the Damage Locations

From the electrical damage picture, the stress must be applied at either the Vbb or VDD pad.

- A positive stress at Vbb could basically explain all three damage points, even if damage point 1 could only be explained if there is a low ohmic connection between VDD and GND; hence a high R_{VDD} could help to avoid the damage (see Figure 68).
- A negative stress at Vbb could explain damage points 1 and 2, but not damage point 3. Again, for damage point 1, a low ohmic connection between VDD and GND is needed and a high R_{VDD} could help to avoid the damage.
- A positive stress at VDD could basically explain all three damage points; the damage will not be influenced by R_{VDD}
- A negative stress at VDD can not generate the damage since the diode at the GND pin is taking the current.

From this analysis it is very likely that either a positive or negative pulse at Vbb or a positive pulse at VDD was the cause. To narrow down possible root causes the customer application was reviewed.

Customer Application

Figure 69 shows the customer application. As mentioned before, one possible cause could be a positive stress at VDD. But since the application had a 5 V regulator on board it was very unlikely that VDD would be touched directly once the board was mounted in the car.

If there is a positive stress to Vbb with a voltage greater than 61 V, or a negative stress smaller than -10 V, a high current will flow, charging up the capacitor C_{VDD}, since no current limiting resistor R_{VDD} was mounted on the board. With this knowledge, the cause could be narrowed down to a negative overvoltage at the battery pin Vbb (e.g. reverse battery, ISO1 pulse or similar) or a positive overvoltage at the battery pin Vbb (e.g. by load dump, ISO2 or similar).

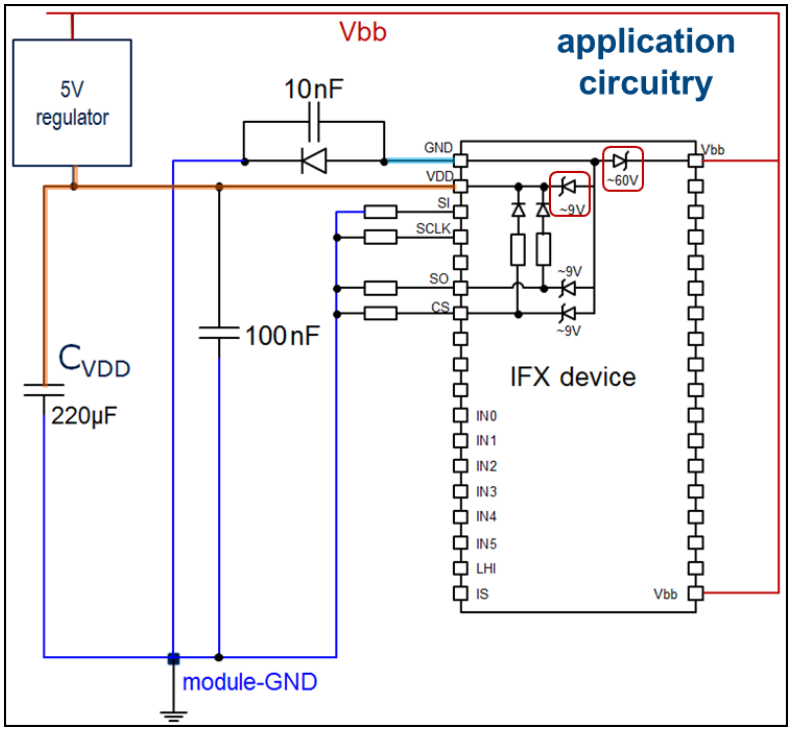


Figure 69: Customer Application

In order to reproduce the damage signature from the field returns, a simplified test board was built with passive components as in the application. The value of the current limiting resistor R_{VDD} was modified while positive and negative voltage pulses were applied to Vbb using a DC power supply and power switch blocked by a capacitor array. The voltages were ramped in small steps and applied as a single pulse until the device was damaged.

For a positive Vbb stress, the device showed comparable damage signatures to the field returns. The damage happened at a stress $\geq$ 41 V with R_{VDD} = 0 ohm and at a stress $\geq$ 49 V with R_{VDD} = 470 ohm.

For a negative Vbb stress, the device also showed comparable damage signatures to the field returns. The damage happened at a stress $\leq$ -10.5 V with R_{VDD} = 0 ohm and at a stress $\leq$ -24 V with R_{VDD} = 470 ohm.

Root Cause/Summary

A missing resistor between VDD and GND created a potential cause for EOS damage. The damage could be reproduced in the lab with positive and negative overvoltage as well as reversed battery operation. The recommended solution was the addition of a current limiting resistor between VDD and GND. Once the recommendation was implemented on the board, no damage was reported.

Note: the root cause of the problem could not be confirmed as one specific event, but the stress voltages used to duplicate the field returns are very common in automotive assemblies.

5.9 Case 9: Supply Capacitor Switching

Failure Occurrence and Failure Mode

A 3-axis accelerometer IC was experiencing an intermittent internal failure rate in testing. The failure was seen as high leakage on input pins as well as elevated supply leakage. The failure was traced to two EIPD sites on the die. One was in a fuse block where fuses were blowing randomly, shown in Figure 70. A second area was in an unrelated logic block (but still powered by the same supply) where an EIPD damage location resembling latch-up was observed as depicted in Figure 71.

SN1540 FA	29	28	27	26	25	24	23	22	21	20
7	0	0	1	0	0	0	1	1	1	1
6	1	1	0	1	0	0	0	1	1	1
5	0	1	0	0	0	1	1	0	0	1
4	0	0	0	0	0	1	1	1	1	1
3	1	0	0	1	0	1	1	1	1	1
2	0	0	1	1	0	1	0	1	0	0
1	0	0	0	0	1	0	1	1	0	0
0	0	0	1	0	0	1	1	0	0	1

Figure 70: Random Fuse Block Failures in an Accelerometer IC

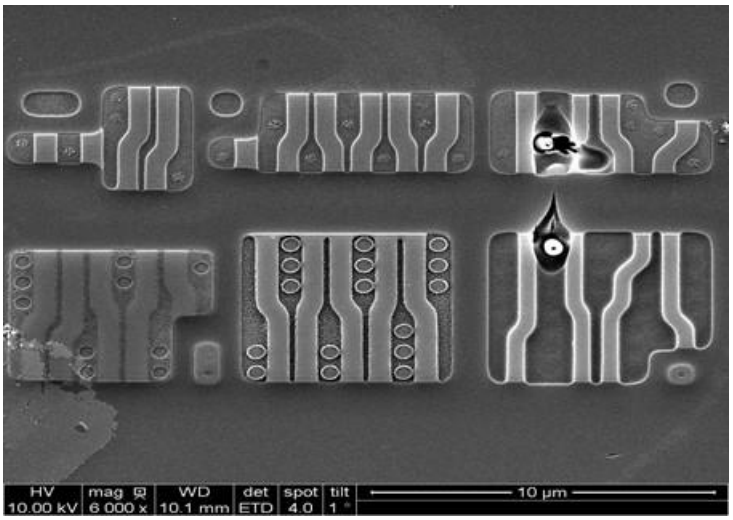


Figure 71: NMOS / PMOS Latch-up Failure in an Isolated Logic Block of an Accelerator IC

Analysis and root cause

Analysis of the layout revealed that the damage resulting in elevated supply current was caused from electromigration of a supply bus within a small logic block. This resulted in shorting of the logic and an incorrect voltage level measurement on the affected input pin. Damage resembling that

of a latch-up failure was also seen within and between the NMOS and P-channel metal-oxide-semiconductor (PMOS) devices of a buffer in this same logic block. This logic block was similar to other isolated logic blocks in the area but was the closest block to the product's supply pin. This provided additional insight as similar logic blocks further away along the VDD bus did not fail.

The component had robust (3500 V HBM and 1250 V CDM) ESD classification test ratings, and the JESD78D latch-up classification test passed 100 mA. As the failures were observed in test, the test board hardware design was analyzed. The production electrical test boards used solid state switches to handle the different setups required of the product testing. These 12 V metal-oxide-semiconductor (MOS) switches leaked a negligible, but non-zero, amount of current, which was normally acceptable. However, in the situation where no device was connected to the test site, the "negligible" leakage current created a condition where it slowly charged a 1 µF external decoupling capacitor (connected between power supply and ground) to significantly above the power supply voltage as shown in Figure 72. This problem was difficult to detect, because when an oscilloscope probe was connected to the VDD line to monitor transients across it, the probe added a small load, giving the leakage current a discharge path and preventing the capacitor from charging. When a device finally entered the test site after a substantial wait time, it was exposed to a transient of up to 12 V in magnitude which discharged into the VDD pin of the device, creating the observed damage as seen on the failure analysis micrographs.

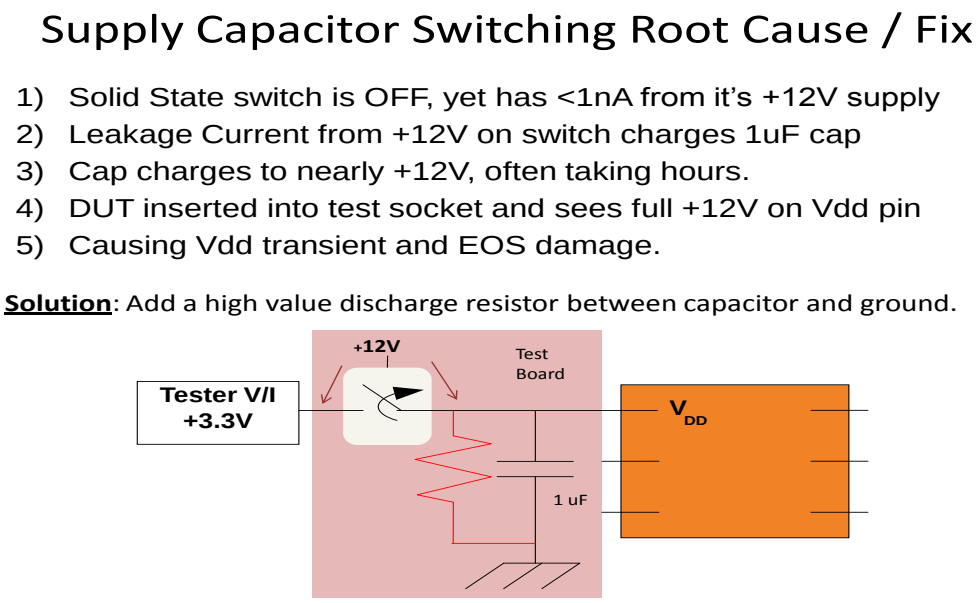


Figure 72: Root Cause and Fix for Supply Capacitor Switching Failure

Solution

The solution was to add a high value resistor to the VDD line (shown in Figure 72). The resistor was chosen such as not to impact current measurement and hence be present by default. To validate that the solution worked, 500 devices were sent through power-down and quality control testing on two testers while monitoring the VDD line with a scope isolated from VDD by a buffer. The high value resistor was added to one tester followed by a long time observation. If the modification addressed the issue, over time only the non-modified tester would see the charging effect. Over the course of a couple hours, results showed that the non-modified tester charged the capacitor resulting in the

discharge, while the modified site capacitors remained un-charged, eliminating the possibility of EOS damage.

5.10 Case 10: CBE in DSP IC

Failure Occurrence

During system level production testing and field application, a customer had a several hundred parts-per-million (PPM) failure rate on a four-level-metal, deep- submicron CMOS DSP packaged in a 28 x 28 mm², 208-lead plastic quad flat pack (PQFP).

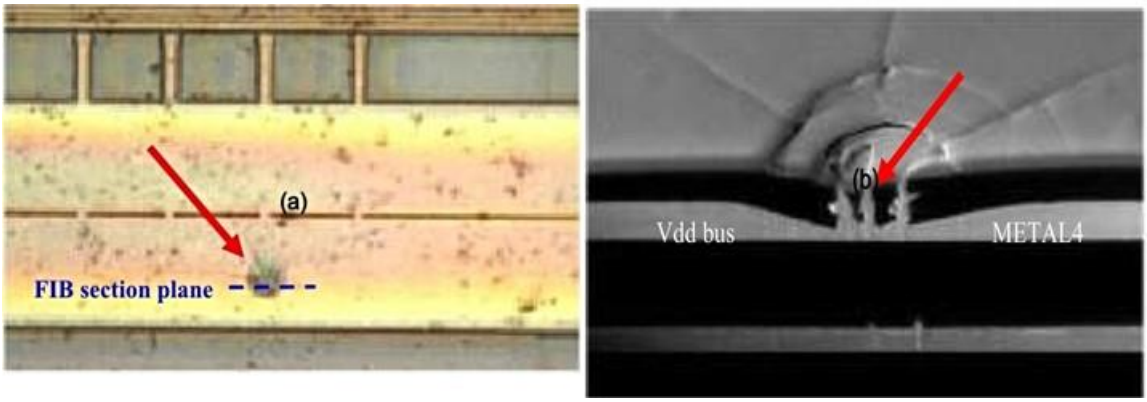
Failure Mode

The failure modes varied, but typically involved functional failures within a small block of circuitry within the DSP.

Analysis and Simulation

The DSP was located near a corner of the PCB above relatively large copper ground planes in both the top and bottom layers of the PCB. All the components were on one side of the customer's four-layer PCB. The top and bottom ground planes were interconnected by numerous plated through-holes. The 35 GND pins on the DSP package were tied to the interconnected copper ground planes, while the 33 VDD pins were tied to an internal copper VDD power plane. The other internal PCB layer was used for routing IO signals.

Failure analysis of samples of the DSP board failures revealed damage at VDD buses in the form of ~10 μm diameter circular areas of melted aluminum-copper (AlCu) with cracked or ruptured overlying passivation (Figures 73 and 74). Banerjee et al [6] have attributed damage similar to that in Figures 73 and 74 to extreme current densities (typically ~5 x 10 A/cm² for AlCu METAL4) during short pulses (~100 ns) such as ESD that heat AlCu to ~1000 °C, well above its melting point. At this temperature, the thermo-mechanical stress exceeds the fracture strength of the overlying oxide-nitride passivation layer, causing it to rupture. As shown in Figure 73, the passivation ruptured in a spider-web-like pattern, and parts of the passivation "caved-in" as the AlCu metal melted and reflowed as vertical "fingers." However, the damage shown in Figures 73 and 74 did not result in the observed electrical failure modes since the VDD buses were not fused open.



Figures 73 (left) and 74 (right): Optical (left photo) and corresponding focused ion beam (FIB) cross-section image (right photo) of the melted / reflowed METAL4 AlCu "fingers" (see arrow) and overlying cracked passivation on a customer DSP board failure.

Further failure analysis of the DSPs that failed in the customer PCBs showed that the functional failures were due to CMOS transistor "stuck at" faults caused by excessive trapped negative charges in the gate oxide of one or more CMOS transistors. This was validated by using a focused ion beam (FIB) to scan the gate oxide of stuck transistors with gallium ions (Ga^+). These positive ions neutralized the negative trapped charges, resulting in functional recovery of the failing transistors. The charge trap sites were generated when the ~12 V tunneling voltage of the gate oxides of these transistors was exceeded. This occurred when the product of the VDD interconnect resistance for these transistors (*Rinterconnect*) and the high current ESD transients (*Ipeak*) in these VDD interconnects was >12 V. Depending on the density of the trap sites generated in the gate oxide and their fill rate during subsequent PCB operation, the DSP time-to-failure ranged from days to months after the ESD events.

Neither HBM nor CDM testing could replicate the relatively severe damage seen on the customer board failures. At the component level, the VDD pins on this DSP in a 208-lead PQFP were extremely robust to ESD events, passing at least 7000 V HBM and 2500 V field induced charged device model (FICDM) testing (Testing was not conducted above these high voltage levels). Decapsulation of samples subjected to these extreme device level ESD events showed no visible damage.

Field induced charged board event (FICBE) testing was conducted using a Keytek Verifier Robotic CDM test system. To assist simulating the failures shown in Figures 73 and 74, the customer provided numerous PCBs. Since the complete customer PCB was larger than the 127 mm (5") field charging plate, the PCBs were cut-down in size. However, the ground plane under the DSP was kept fully intact. (Note: More complete details on the customer's PCB design were not provided since this information was proprietary.) Since full electrical testing of the cut-down PCBs was not feasible, the DSP on each PCB was decapsulated to expose the die for visual inspection purposes. Initial high-magnification die inspection of the DSPs on the PCBs revealed no anomalies like those shown in Figure 73.

The FICBE test method for each customer PCB was as follows:

1. The cut-down PCB was centered on the charging plate (see Figure 75). Fortunately, the PCB had no components on the bottom side, so it rested flat on the charging plate. In this configuration, the capacitance measured between the PCB ground planes and the charging plate was ~420 pF, while the capacitance between the PCB VDD plane and the charging plate was ~460 pF.
2. The charging plate was raised to +125 V and then the ground plane was discharged at a test pad close to the edge of the PCB. This was repeated two more times.
3. High magnification optical die inspection was conducted to look for the onset of damage.
4. The charging plate was brought to –125 V and then the ground plane was discharged at the same PCB location. This was repeated two more times.
5. High magnification die inspection was again conducted to look for the onset of damage.

Consistent with the procedure in Steps 2-5, the ground plane on the same PCB was subjected to FICBE testing in 125 V charge voltage increments until high-magnification optical inspection revealed damage.

Figure 75: FICBE test method setup for the cut-down customer production board with the decapsulated DSP. The cuts were made along the top and left side of the PCB. Note that the DSP is located near the original corner of the PCB.

For three PCBs that were CBE tested as per the previous paragraph, the DSPs showed VDD bus damage similar to that in Figure 73 after the 250 V stress. FIB analysis of these CBE failures consistently showed ~10 μm diameter circular areas of melted or reflowed AlCu with cracked or ruptured overlying passivation (see Figure 76). Thus, FICBE testing successfully replicated the real-world board failures (Figure 74).

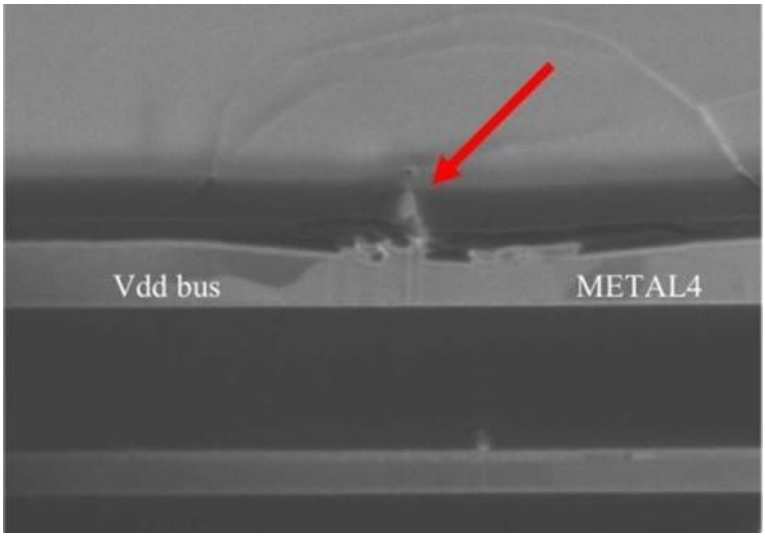


Figure 76: FIB cross-section image of the melted and reflowed METAL4 AlCu (see arrow) and cracked glassivation on a DSP IC stressed at -250V CBE using the setup in Figure 75.

The DSP's 35 GND pins and 33 VDD pins soldered to the PCB provided very low inductance and resistance connections between the DSP and the PCB ground and VDD planes. To qualitatively determine how much this affected the CBE ESD results, the testing was conducted on two sets of cut-down PCBs:

1. **Controls**: Two PCBs with all 208 pins on the DSPs soldered to the board, including all 35 GND pins and 33 VDD pins.
2. **Single Supply Pins**: Two PCBs as above, except all but one GND pin and one VDD pin were mechanically cut away so that they no longer contacted the PCB power planes.

CBE testing was conducted as detailed above starting at ±125 V with 125 V increments. To minimize the time required to inspect the DSP die after the PCB stressing at each voltage level, the inspection failure criteria was revised to be catastrophic damage readily visible during low magnification optical inspection as shown in Figure 77. Results of this testing are provided in Table 6.

Table 6: Testing Results

Pins Soldered to PCB	Pass	Fail
35 GND's + 33 VDD's	875 V	1000 V
1 GND + 1 VDD	1125 V	1250 V

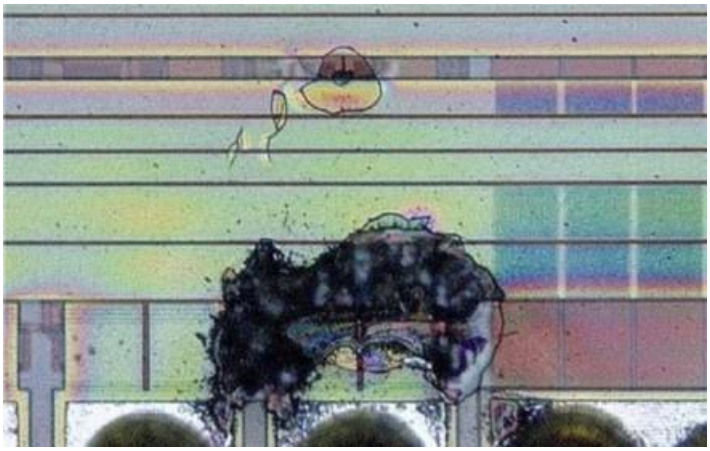


Figure 77: Typical catastrophic DSP damage observed along the supply buses and adjacent bond pads after stressing the cut-down customer boards at the CBE fail voltages listed in Table 6. Note the large areas of melted AlCu and missing passivation above this damage.

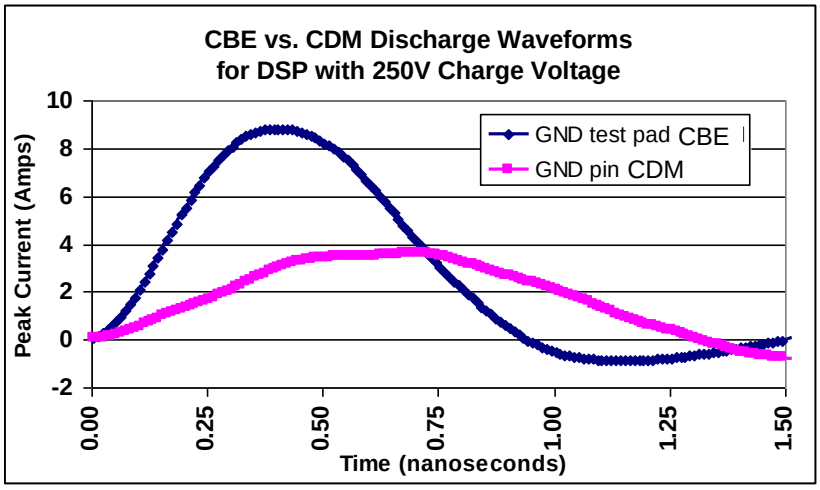


Figure 78: Comparison of 250 V FICBE and FICDM discharge waveforms at a DSP ground pad and pin depicting the higher energy in the CBE event for the cut-down PCB shown in Figure 75.

During component level CDM testing of the DSP in a 208-lead PQFP package, the capacitance measured between a VDD pin and the charging plate was ~25 pF. However, during CBE testing of this IC on the cut-down customer production board shown in Figure 75, the capacitance between the VDD plane and the charging plate was ~460 pF. Thus, for a given charge voltage, the peak current during a CBE discharge was much higher than a CDM discharge. This can be seen in Figure 78 which shows a comparison of the 250 V discharge waveforms at a ground pin on a stand- alone DSP (i.e. an FICDM discharge) versus a GND test pad when the DSP was on the cut-down board (i.e. an FICBE discharge) with all 35 GND and 33 VDD pins connected to the PCB power planes. Note that the board discharge waveform has a faster rise time than the device discharge waveform due to the lower inductance and resistance of the board discharge path.

Based on the construction of the production board PCB, when the charging plate was charged negatively during FICBE testing, a positive charge was induced on the ground plane on the bottom of the production board and a negative charge was induced on the internal VDD plane above this ground plane. When the ground plane was discharged (i.e., grounded), much of the negative charge stored by the VDD plane on the PCB was channeled through the DSP since it provided such a low impedance path to the ground plane. During this specific discharge event, this low impedance was due to the combination of the following factors:

- The 33 parallel VDD pins on the DSP package that were connected to the VDD plane provided a much lower inductance and resistance discharge path between the VDD plane and the DSP than any other IC on the PCB. (Other ICs on the PCB had only one VDD pin tied to the VDD plane.)
- The DSP has a large die with $>10^5$ parallel forward-biased diodes formed between the N-wells tied to VDD and the large P- substrate tied to GND. These $>10^5$ parallel diodes provide a far lower "on" resistance (only ~0.2 Ω) during high-current, forward-biased operation than any other diode paths on the PCB.

- The 35 parallel GND pins on the DSP package that were connected to the ground plane provided a much lower inductance and resistance discharge path between the DSP and the ground plane than any other IC on the PCB. (Other ICs on the PCB had only one GND pin tied to the ground plane.)

The combination of the above factors caused the DSP to be the primary CBE discharge path between the negatively charged PCB VDD plane and the PCB ground plane when it was grounded during the CBE event. Thus, the charge voltage required to damage the DSP's VDD buses at the board level (i.e. -250 V) was <10% of that required to cause such damage at the component level (i.e. >2500 V).

As expected, the CBE ESD withstand voltage of the DSP was higher when only one GND and one VDD pin were connected to the PCB (Table 6). This is because single supply connections increase the inductance and resistance of the discharge path through the DSP and consequently more of the CBE ESD current flows through other components on the PCB.

Root Cause

Investigation of the customer's board assembly process showed that the DSP on the PCB was sometimes charged to at least ±300 V prior to wave soldering. Much of this charging was caused by the prior manufacturing step in which large plastic edge connectors were attached, resulting in inductive charging of the PCBs. Subsequent wave soldering instantaneously discharged the DSP and all other components on the PCB.

Solution

As a corrective action, the customer added an ionizer to their production line just prior to wave soldering to safely dissipate charges on the PCB. No ESD related DSP damage has occurred subsequently, thus proving the effectiveness of this corrective action.

5.11 Case 11: Reliability Testing

Introduction

In this section we describe a transient triggered active MOSFET rail clamp instability observed on clamps for 5 V power rail protection. This instability led to a few devices with severe EOS damage during product burn-in (BI). The fundamental issue here was that the lateral NPN bipolar holding voltage (V_{hold}) for the 5 V NMOS clamp transistor as initially implemented in layout, was a bit below the 6.0 V supply level used for BI (V_{BI}). It is well known [7, 8] that this is a dangerous condition as the clamps, once fired, may latch with sustained high current. Here we define V_{hold} as the minimum voltage for which lateral NPN bipolar conduction can be sustained. To avoid any confusion with traditional latch-up involving the silicon controlled rectifier (SCR) inherent to CMOS, we use the term "powered bipolar latching" (PBL) to describe this phenomenon.

Discovery at Burn-In

A product processed in a 90 nm bulk CMOS technology utilizing 5 V resistor capacitor (RC)-triggered active rail clamps suffered power supply interrupts during 150 °C BI testing with V_{BI} set to 6 V. Details of the ESD network design can be found in [9]. Typically one or more units on a board suffered massive EOS damage primarily centered over the 5 V ESD clamps (see Figure 79). Failing clamps were associated with isolated supply domains (e.g. VDDA) with minimal on-chip decoupling capacitance. There were no failures observed when V_{BI} was set to 5.8 V or lower. False triggering of the ESD clamps during power supply ramp-up was initially suspected, but the power up slew rate during BI was well controlled and extremely slow (~1 V/s). Furthermore, the failures occurred several hours into BI testing. It was therefore suspected that the clamps must be firing due to voltage spikes during BI on the powered VDDA supply.

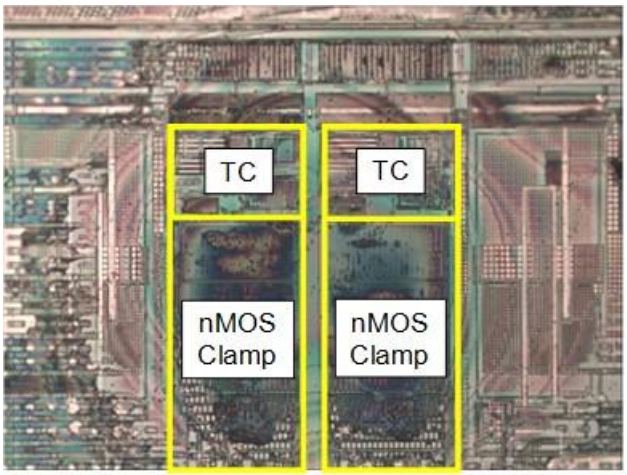


Figure 79: Photo of EOS Damage in 5 V ESD Clamps after BI

In an attempt to reproduce the PBL behavior leading to clamp failures during BI, a series of bench measurements on packaged units was performed. The device under test (DUT) was placed on a test board and heated to 150 °C. The VDDA supply was ramped from either ground, or an initial voltage level, with a low impedance variable slew rate pulse source (see Figure 80). Oscilloscope probes

were connected on either side of a series resistor between the pulse source output and the DUT to provide an indication of current flow.

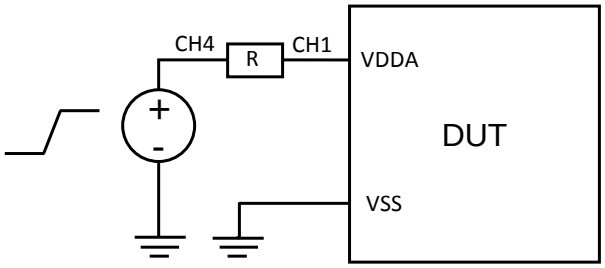


Figure 80: Characterization Bench for ESD Clamps.

Figure 81 illustrates a typical measurement result for the product. Scope waveforms on the supply are shown. The two waveforms on the plot correspond to the voltage before (CH4) and after (CH1) a small (4 ohm) series resistor. In this example the supply was ramped from 0.8 V to 6 V with a "fast" (~20 kV/ms) slew rate. Note that the ESD clamps initially fire in MOS mode, as the timing circuits (TCs) respond to the fast ramp, and then show the expected time-out after about 10 µs. This pin on the DUT is protected by two large clamps wired in parallel each having its own timing circuit (TC), and placed in adjacent power/ground pads. The two clamps can be seen to exhibit slightly different time-out intervals due, it is assumed, to a slight difference in the TC supply voltage. With both clamps firing in MOS mode, a total current of about 400 mA is drawn through the series resistor. This current drops to about 200 mA after the first clamp times out.

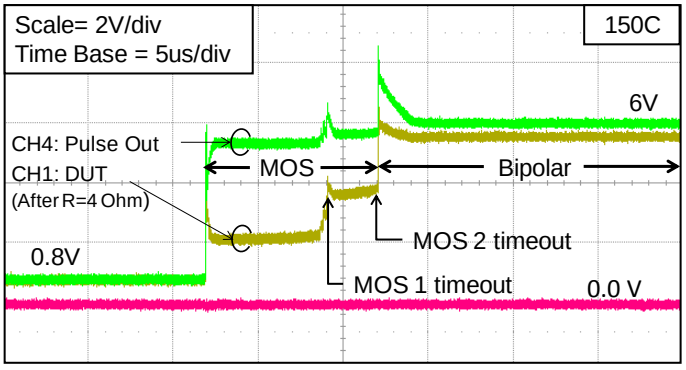


Figure 81: Fast VDDA Slew Rate resulting in MOS Clamp Conduction and Subsequent Triggering of Parasitic Bipolar

A key point to note on this plot is that, as the second clamp times out, the clamp current does not show the expected drop to zero. Instead a sustained current draw of about 50 mA is observed with 6.0 V on the supply (CH4) and 5.8 V on the DUT pin (CH1). Slew rates below the TC trigger threshold failed to produce this sustained current flow. TLP on powered on structures [5] showed that the trigger voltage is below 8V and that with DC bias >4V the clamp did not trigger into MOS mode conduction, but only turned on in bipolar mode.

These measurements among others provided a clear picture of events leading to the 90 nm product BI failures. A noise spike on the DUT VDDA pin during 6 V BI likely initiated sustained PBL, leading to the observed EOS damage. With a minimum V_{hold} of approximately 5.7 V (as measured by powered TLP [5]), this was clearly a risk.

A review of the layout of the large 5 V clamps in the power/ground pads of the affected product showed that intermediate well ties between banks of NMOS fingers were not well strapped to VSSE. Layout fixes to reduce the interconnect resistance improved the clamp V_{hold} above 6 V, and no further failures were seen in BI. However, for future designs it was desirable to build in more margin to PBL in order to account for process variation and drift. The subsequent section describes how this was achieved at the 55 nm technology node.

V_{hold} Engineering

As a result of the PBL marginality seen during BI in the 90 nm technology, design options were explored in a 55 nm bulk CMOS technology to adjust the V_{hold} of the 5 V clamp.

In order to evaluate the clamp options, an IO test chip was designed with multiple instances of power and ground cell pairs in which full-size resistor capacitor (RC) clamps were implemented.

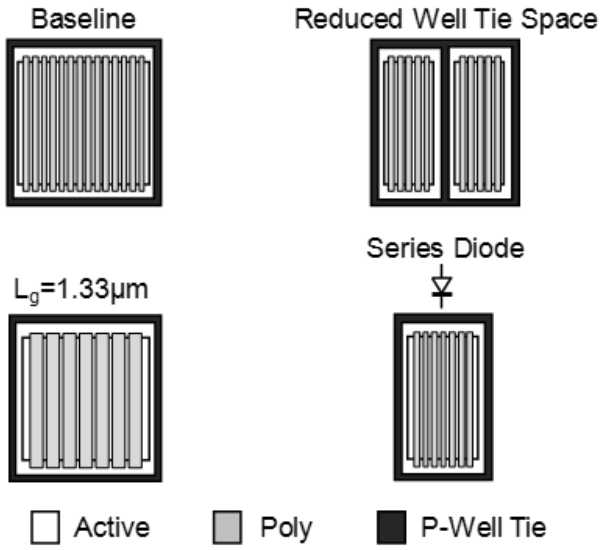


Figure 82: Layout of the Clamp Unit Cells

Three options (Figure 82) were designed to increase V_{hold} over the baseline clamp. Each of the clamps was implemented in the same cell floor plan as the baseline clamp so that the layout areas are nearly the same. The first option, referred to as the "reduced well tie space" clamp, was implemented with a well tie space (parallel to the poly orientation) of exactly one half of the baseline clamp. The reduced well tie space decreases the base resistance and should therefore increase V_{hold}. The second option, referred to as the "Lg=1.33 µm" clamp, increased the channel length of the constituent 5 V NMOS transistor. This option increased the base width of the lateral NPN bipolar of the 5 V NMOS transistor, reducing its gain, which should have also increased V_{hold}. The third option, referred to as the "series diode" clamp, included a diode in series with the NMOS clamp transistor. For this option, the voltage drop of the series diode resulted in an effective V_{hold}

increase for the diode/NMOS combination. The diode was implemented such that its I_{t2} was always greater than that of the series NMOS.

TLP Measurement Results

Comparison of the clamp options described above involved not only the V_{hold} but the costs associated with each option. These costs included both the impact on ESD self-protection and layout area in each case. Three metrics were considered for comparison: (1) the increase in V_{hold} over the baseline; (2) the MOS mode conductivity; and (3) I_{t2} of the clamp element in the CDM time regime, where (2) and (3) are normalized to layout area.

The powered TLP technique described in [5] was utilized to determine the V_{hold} of the clamp options, whereas the MOS conductance and 1.2 ns I_{t2} were extracted from traditional unpowered TLP curves. The results of these measurements are summarized in Table 7.

Table 7: Summary of Clamp Option Metrics

Clamp Structure	V_{hold} (V)	MOS Conductance ($mS/\mu m^2$)	1.2 ns I_{t2} ($mA/\mu m^2$)
Baseline	5.9	0.065	> 1.3
Reduced Well Tie Space	6.4	0.064	1.1
Lg=1.33um	7.1	0.039	0.74
Series Diode	7.5	0.060	> 1.3

From Table 7 it is clear that the baseline and series diode structures performed best in terms of I_{t2} during unpowered 1.2 ns very fast transmission line pulse (VFTLP) testing, as both reached the limit of the tester before failure.

Solution

Clearly, the series diode produces the largest increase in V_{hold} over the baseline clamp. More importantly, the costs associated with this increase are minimal: when compared to the baseline structure there is no practical degradation in the area normalized MOS conductance or the 1.2 ns I_{t2}. For these reasons, the series diode option was chosen as the preferred clamp element in this technology.

5.12 Lessons Learned

The case studies have shown that there are many different ways to encounter EOS damage in products. They also illustrated that it is often difficult to find a completely explained root cause for the observed problems. ***A full root cause analysis is only possible with very good cooperation between supplier and customer.***

All case studies showed that damage occurred because the system/IC was brought into an unforeseen situation where it was stressed outside the specified range. In some cases, this was simply a consequence of mistakes. In other cases it was caused by phenomena that were not considered during the design of the product or during the design of the assembly process.

The case studies also showed that very often it is possible to find controlled stress experiments that replicate the observed damage. This is very helpful in understanding possible root causes and potential solutions. Several examples demonstrated the usefulness of the power profile. It defines the safe operation area for a certain pin as a function of stress time, or in other words, the minimum power required to inflict damage as a function of duration of that power. At the same time, it provides a means to obtain reference failure signatures. In [1] it is shown, both on test structures and on the product level, that stress considerably above the level set by the power profile, leads to very comparable yet more severe damage. Thus, it is often already visible without detailed failure analysis. This is probably one of the reasons for the often used method to classify customer returns as EOS or ESD returns without addressing the root cause that actually has led to the damage.

The above analysis implies that multiple people are responsible for a successful end-product. Marketing engineers of suppliers and customers need to agree on reasonable specifications. IC design needs to make the design such that the power profile is not below the agreed specifications. The IC manufacturer needs to produce the design and verify during IC qualification that the design meets the agreed specifications. At the same time, the system designer needs to ensure that under normal user and test conditions, components used in a system are not brought outside the SOA. The system manufacturer needs to take precautions in system assembly, testing, application and handling to never exceed the power profile. Finally, the end-user has the responsibility to not use the finished system outside the specified normal range of operation.

If all is implemented correctly, a consequence is that all damage induced by electrical stress is EOS damage. This is completely in line with the fishbone diagram presented in Chapter 4. This philosophy does not imply anything about which level is correct (or not) or which level is justified or not for any of the parameters. It just states that once a design has been shown to meet the agreed specifications, any electrically induced damage must be EOS - the product was stressed beyond its agreed limits. Typically, it is not possible to conclude on *how* and *why* this happened without a close cooperation between supplier and customer in the root cause analysis.

5.13 Conclusions

This chapter presented 11 case studies of EOS damage with as complete a root cause analysis as possible. It has been shown that often the failure signature and damage can be replicated by controlled experiments. The chapter also demonstrated that, in general, EOS occurs when products are brought outside their specification limits. The reasons why this happens and the mechanisms of how this happens can vary widely. It is clear that adequate solutions to EOS problems are only possible through thorough understanding, which is possible via a root cause analysis where all parties cooperate on the same level.

References

[1] T. Smedes, Y. Christoforou and S. Zhao, ‘Characterization Methods to replicate EOS Fails’, Proceedings EOS/ESD Symposium, pp. 384-392, 2014

[2] ZVEI, ‘First-Mate-Last-Break grounding contacts in the automotive industry’, White paper, 2011

[3] A. Righter, E. Wolfe, J-J Hajjar, ‘Non-EOS Root Causes of EOS-Like Damage’, Proceedings EOS/ESD Symposium, pp. 312-317, 2014

[4] A. Olney, B. Gifford, J. Guravage, A. Righter, “Real-World Charged Board Model (CBM) Failures”, EOS/ESD Symposium Proceedings, pp. 34-43, 2003
[5] R.S. Ruth, ‘Investigation of Product Burn-in Failures due to Powered NPN Bipolar Latching of Active MOSFET Rail Clamps’, Proceedings EOS/ESD Symposiu, pp. 313-322, 2013
[6] K. Banerjee, D-Y Kim, A. Amerasekera, C. Hu, S. S. Wong and K. Goodson, “Microanalysis of VLSI Interconnect Failure Modes Under Short-Pulse Stress Conditions,” IEEE International Reliability Physics Symposium, pp. 283-288, 2000.
[7] F. Farbiz, A. Salman, G. Boselli, “Novel Technologies to Modulate the Holding Voltage in High Voltage ESD Protections,” EOS/ESD Symposium Proceedings, pp. 69-75, 2011.
[8] N. Peachy, R. Gauthier, R. Phelps, E. Gebreselasie, “Transient Latch-up of Switching Arrays in Power Management Circuits,” EOS/ESD Symposium Proceedings, pp. 152-160, 2012.
[9] S. Ruth, M. Stockinger, J. Miller, V. Whitney, M. Kearney, S. Ngo, “A CDM Robust 5V Distributed ESD Clamp Network Leveraging Both Active MOS and Lateral NPN Conduction,” EOS/ESD Symposium Proceedings, pp. 7-15, 2011.

Chapter 6: EOS Analysis and Diagnosis - "Techniques and Methods for Dealing with Electrically Induced Physical Damage"

David Eppes, Advanced Micro Devices
Leo G. Henry, ESD/TLP Consulting
Tim Maloney, Intel Corporation
Jim Vinson, Intersil

6.0 Introduction

This chapter will provide a basic summary of the typical process flow and methods for analysis of component electrical failures, with an emphasis on determining the cause of damage induced by electrical overstress. Guidance on increasing the probability of successful determination of root cause is also covered in the chapter, including the concepts of customer and supplier information exchange optimization and avoiding secondary electrical damage. Challenges faced by failure analysts and misconceptions about FA on the part of both customers and suppliers are included in the chapter. While failure modes resulting from electrical overstress damage will be discussed, soft failure and system upset will not be addressed as part of this chapter. The chapter concludes with a discussion of EOS failure mechanisms and causes, which can assist in determination of root cause.

6.1 Optimal Customer and Supplier Failure Symptom Information Exchange and Device Handling

When a device is damaged in a system, both customers and suppliers want to know why. Since both parties have a mutual interest in determining root cause so that future failures can be eliminated, it is important for suppliers and customers to work together on resolution.

Defects, misapplication, and electrical overstress account for a significant percentage of failures, and all three can initially display identical symptoms. While the supplier has in depth knowledge of the supplied component, the customer has in depth knowledge of the history and application of the device prior to failure. Determination of root cause is always made easier when information is shared openly between suppliers and customers. What is needed by a supplier to pursue an investigation includes the following information and questions answered:

- Thorough documentation of the operating state of the component before EOS occurred and any symptoms of failure. This includes component operational "states" and physical system observations (such as unusual functionality, failed power supplies, or overheating observations) when the failure occurred.
- What were the circumstances surrounding the damage – temperature, bias conditions, atmospheric conditions, type of environment (lab, field, lightning storm, etc.)?
- What specific electrical symptoms were observed and recorded at the time of the damage? (i.e., comprehensive electrical analysis or ATE test, loss of signal output, leakage increased, wrong logical state, gain low, etc.)?

- Were there other components in the system that were damaged? This includes passives components, power supplies and, in particular, components interfacing directly with the returned component?
- If devices from other vendors are used in the system, did they get damaged?
- How were the returned components verified as being damaged (Substituion of failing component with a known good component , electrical test analysis, etc.)?
- How was the device removal accomplished (i.e., desolder, mechanical methods, etc.)?
- Was the damage verified as a particular integrated circuit or other device? If so how?
- Are all electrical test data and symptoms documented?
- Was the device subjected to any known electrical or mechanical disturbances? (Lightning storm, system dropped, power distribution issue, etc.)?
- Was the system checked thoroughly for damage or loss of functionality after the EOS damaged component was replaced in the system?

Once failure is detected, it should be recognized that continued operation of the failing component can lead to enough secondary damage to make root cause diagnosis more difficult or impossible. Admittedly, EOS damage can occur so fast that it is impossible to limit the damage. And some electrical operation may be needed to confirm failure after damage is suspected. But sustained electrical operation after damage should be avoided if possible. This means manufacturers can help suppliers improve success rates for root cause diagnosis by minimizing the amount of time a component is exposed to damaging conditions if it is known to have EOS damage.

6.2 EOS FA Challenges

6.2.1 Description and Interpretation of EOS Damage Modes

EOS is not an infant mortality mechanism (defect driven) and it is not a wearout type mechanism (long term degradation failure). EOS typically does not involve a gradual degradation. Instead, it tends to be more of an event driven mechanism that causes a measurable change in the device. EOS occurs when some event, such as an over voltage pulse, enters the system causing electrical breakdown of a component resulting in physical damage.

Component failure due to EOS can manifest itself in many different ways. Operationally, the effects of EOS can range from performance degradation to catastrophic functional loss. These effects are determined by the amount of circuit damage the device sustained and the sub-functions of the device that are damaged by the EOS event. The level of circuit damage is determined by the duration and energy (i.e., voltage and current) of the event that caused the damage.

6.2.2 Recognition of EOS – What is and what is not EOS?

EOS is not caused by operation of a component within Absolute Maximum Ratings. Typically, something interfacing with the device such as applied power or signal inputs needs to break down, short out or be improperly applied to get the excessive current needed to cause damage. EOS damage has a wide range and can be described as mild, medium, and heavy. EOS stress can range from high power short duration that may fuse open a thin film resistor to low power long duration events that can melt the package. All are EOS but the degree of damage and volume of damage will be vastly different.

Physical symptoms range from an individual transistor suffering gate oxide integrity loss to overheated resistors to substantial movement of the metal films in the vicinity of a damage site. In addition, secondary damage unrelated to the original cause of failure can also be induced if system malfunction is catastrophic and the system remains powered up after damage occurs. Secondary transients may also occur when high current EOS events cause a metal line to fuse open. The inductance in the current path produces an inductive voltage transient due to the fast change in current when the line fuses open. This voltage transient can cause secondary breakdown damage.

6.2.3 Customer Expectations and Misconceptions on Root Cause

When a component fails in a customer application, it is natural to initially assume it is the supplier's issue. While this may be the case, resolution of a electrically induced physical damage condition in a component is best achieved through collaboration between the customer and the manufacturer.

When a customer reviews a manufacturing process and sees nothing wrong, it is easy to believe the EOS could not have occurred in one's facility and is the fault of the supplier. While this can be a valid assumption, damage can be induced in system manufacturing and components can be misapplied without the knowledge of the end user. EOS events typically involve a small percentage of manufactured systems, and can be sporadic in nature. Just because everything is normal in a manufacturing process at the time of inspection does not imply that it was always correct. It is important to review the manufacturing process with an eye on what could go wrong and not what the normal operating process is at the moment.

Manufacturers may also be prone to assuming a customer damaged a returned device with EOS. After all, the device tested out good before it was shipped. But manufacturers also need to recognize that customers may have operated the device within documented requirements, or at least to the best of their knowledge, and that they may be doing nothing incorrectly.

Ultimately, finger pointing between user and supplier about whose "fault" it is turns out to be the worst mode of operation. *Both parties need to work together to resolve the issue and determine root cause.*

6.2.4 Customer Misconceptions about Interpreting FA and the Level of Difficulty

Some customers believe that by simply sending a device back to the manufacturer they will receive an answer to what caused the failure and how to prevent it. Unfortunately, this is rarely the case. Some devices may be too damaged to determine the cause. In other cases, the customer could not provide sufficient information to draw conclusions from the FA, so the manufacturer can only describe the symptoms of failure. And sometimes the manufacturer can determine the most likely cause of failure, but it can't be duplicated in the customer environment (i.e., it may be an isolated event that never occurs again).

If EOS damage were commonplace in manufacturing there would be established protocols for dealing with them. EOS can occur repetitively when assembly lines are ramping up, or EOS can occur infrequently in an established manufacturing line, with the latter case typically being harder to resolve. In addition, there may be more than one cause. While inspecting an assembly line may reveal possible causes, a systematic and comprehensive investigation is typically needed to determine full root cause.

6.3 High Level Preparation Guidelines for Diagnosing the Cause of EOS

The success of a background review is dependent on the quality of the information available and how it is interpreted. If possible this review should include information from both the customer and the supplier. The items customers can provide that are useful in preparing to perform an analysis on failures exhibiting EOS damage include the following:

- a detailed description of all handling steps the device went through from the time it was received to the time a failure was detected
- a detailed description of the system and component failure symptoms
- a description of system functionality after swapping the device with a fresh device (if possible)
- system datasheet
- system schematics and board layout diagrams
- power sequence and system initialization timing diagrams
- a reference functional system if the customer can provide one
- as much background information as the customer is willing to share; it is hard to provide too much information.

Items the manufacturer should gather in preparation for an analysis include the following:

- all customer feedback
- device electrical datasheet or operational specification
- design database (layout and schematic)
- bonding diagrams and package information including package pins and connection maps
- a functioning reference system, if available.

6.4 Failure Analysis Techniques and Procedures

Failure analysis of any silicon failure is a multi-step process. Many of the techniques used for analysis of defects and failures induced by accelerated aging tests can be applied to failures exhibiting EOS damage. The basic steps that can be applied to failure analysis job are:

1) identification and documentation of the basic symptoms of failure
2) system diagnostic testing, if possible, based on the level of damage
3) basic automated test equipment (ATE) test of the returned device, if possible; if an ATE is not available, simple bench testing can be used as an alternative
4) ATE diagnostic, if diagnostic routines are available, to obtain more extensive information about the symptoms revealed in the basic ATE test
5) non-destructive analysis using packaging and physical silicon diagnostic tools to validate initial conclusions derived from test/characterization and also to define the area of damage.
6) physical analysis that is typically destructive to validate conclusions from test, characterization and physical diagnosis; physical analysis can include (but is not limited to) physical imaging of the damage and elemental analysis to gain additional information that complements physical imaging.

6.4.1 Identification and Documentation of Failure Symptoms

Manufacturers often receive EOS damaged devices with almost no documentation of failure symptoms. If, however, the system manufacturer has provided detailed information about the nature of the failure, it may be possible to skip some of the initial analysis steps such as the ATE test. This could be particularly useful when there is a possibility of causing additional electrical damage by testing the unit.

Manufacturers should also physically inspect devices for obvious signs of damage or anomalies and document all findings. This could include inspections for the following:

- burn marks and/or discoloration of the package, die, passives and electrical connections
- slivers, stringers or any conductive material that could short external connections
- mechanical damage which could account for the EOS such as bent pins or smashed solder balls

6.4.2 System Level Operational and/or Diagnostic Characterization

If insufficient information is gained by the failure identification and documentation process, system level diagnostic testing may be required. Diagnostic testing can be performed using the original system, if the system supports it. Boundary Scan and joint test action group (JTAG) are examples of diagnostic tests that are often available on systems.

System diagnostics may require installation of software or diagnostic boards in order to narrow down causes of failure. When performing diagnostic testing, precautions should be taken to avoid secondary damage, if possible. Some components will be totally non-functional, which minimizes diagnostic analysis capability. Others will be partially functional, allowing potential failure locations to be eliminated or identified using system or ATE diagnostics. The degree of damage and the sophistication of diagnostic tools will dictate the best method for diagnostic analysis.

The usefulness of information provided by system diagnostics can range from minimal to detailed. Conclusions that can be drawn from system diagnostics can range from very few to the identification of a failing function that the supplier can then use to narrow down root cause. System diagnostics should of course be used if available.

6.4.2.1 Basic ATE Test

The initial test of a device often involves use of standard production screening methods to validate that a device is fully functional and meets all datasheet specifications and requirements. ATE testers are typically used for this purpose, although some manufacturers may use other methods. For the purposes of this paper, the initial test will assume the use of ATE testers.

ATE testers are programmable systems typically used to control a component and measure its response under varying operating conditions. The sophistication of an ATE test program varies by device and supplier. Some analog and digital signal processing components may only need to apply controlled input signals and measure the output response. Other ATE testers are more complex and assume functional control of components by applying direct stimulus either by functional vectors, analog signals, or machine language instructions to the component. Sub components such as signal generators are used to apply the instructions while power supplies control the voltage and current to the supply rails. Response is typically measured with signal analyzers that precisely measure signal

voltage and current as a function of time to evaluate the component functionality and performance, while voltage/current detectors built into power supplies monitor applied voltage and current.

Most ATE test programs include basic parametric analysis of supplies and IOs. Parametric testing is often performed at the beginning of the program. These tests serve at least three purposes:

- verification of good electrical continuity to the component
- detection of shorted pins that could cause damage to the ATE tester or component if full voltage were applied to the pin
- identification of leaky, shorted or open supplies and IOs for diagnostic purposes.

Since opens, shorts and leaky pins are modes of failure that can be exhibited by EOS damaged devices, some failures are detected very early in the ATE test. Once shorts are detected, care should be taken to not create additional damage to a component with extended operation. While the ATE tester can provide additional information on the nature of the failure if the device is tested functionally, engineering judgment should be used to avoid creating secondary damage that obscures the determination of possible root causes. Precautions range from use of current or voltage clamps to discontinuing any further ATE testing.

Many ATE programs perform functional tests after parametric testing. If a device passes parametric analysis but EOS is still suspected, functional testing can often reveal additional clues on the nature of the EOS damage. Since functional testing can also induce secondary damage, it is often desirable to limit the amount of functional testing by avoiding repetitively applying the same test. Shmoo plots are an example of a repetitive test that can cause secondary damage since it intensively exercises a failing condition, but simply running a device multiple times can also lead to secondary damage.

6.4.2.2 ATE Diagnostic Software

Since many failures exhibiting EOS damage are associated with damage to power supply pins or interface pins, some of the diagnostic tools typically used for diagnosing defects deep in an IC may not be needed. But EOS can expose weaknesses or defects that would be benign if not exposed to overvoltage; and diagnostic tools can also be used to exercise a device during physical fault isolation, which will be discussed later.

ATE based component diagnostic software tools have varying degrees of sophistication. Some of the commonly used tools used are JTAG, built-in self-test (BIST) and automatic test program generation (ATPG).

- **Boundary Scan and JTAG** was originally developed as a board/system debugging tool that followed an industry standard protocol. Many integrated circuits also have Boundary Scan and JTAG functions built into them that can be accessed by the ATE tester as well. These functions can be used as debugging tools to take direct control of blocks or macros in an IC, stop operation at a specific instruction and directly access data storage sections of an IC such as the caches or data registers.

- **Built-in self-test (BIST)** is a reference to system or IC component self-evaluation tools that are often used in conjunction with JTAG for diagnosis. State machines within an IC component can be used to sequentially control blocks or macros to perform the self tests. One

of the more common forms of BIST on an IC component is memory BIST, which is used to evaluate the integrity of memory arrays in the IC.

- **Automated test program generation (ATPG)** is a common reference to a tool that identifies failing logic sub-circuits. Use of these tools on an ATE tester typically involves preconditioning the component to a known state. Once in the known state, several clock signals are applied to "toggle" the circuits. After toggling, the state of the sub-circuits are streamed out in a controlled fashion that detects when sub-circuits are in abnormal states. Often a software post processor or manual design analysis are then used to provide a prediction of which sub-circuit or circuit element is failing.

If and when a failing circuit is identified with ATPG tools (or any method for that matter), it is good practice to employ physical fault isolation methods to validate these locations. Physical fault isolation is described in the next section.

6.4.3 Non-Destructive Fault Analysis

After testing and electrically diagnosing a device, some failure analysts may decide to proceed with destructive physical analysis of a suspected area of damage. While this can sometimes save time, there are several reasons not to proceed with destructive analysis without first performing non-destructive fault isolation.

- Physical failure analysis can also be a very time consuming and expensive process requiring specialized hardware and extensive training to do properly. So if a decision is made to proceed with physical analysis, it is best to have a high degree of certainty in the location of the damage.
- Once destructive anlysis begins, it becomes much more difficult if not impossible to perform any addtional non-destructive analysis.
- Suspected areas of damage can be confirmed with non-destructive fault isolation and additional, sometimes unexpected, information can be gathered about the nature of the damage location.
- Non-destructive analysis can save time in the long run and, in some cases, eliminate the neeed for destructive analysis.
- Non-destructive analysis increases the probability of success in the destructive analysis.

Tools exist for performing both package and die level fault isolation. Section 6.4.3.1 will discuss package level fault isolation. Die level faults can create package level symptoms that point to defects in the die, so package level fault isolation is often used. The electrical fault isolation tools, discussed in Section 6.4.3.2, are then used to narrow down the location of damage to as small an area as possible without physically damaging the device further.

6.4.3.1 Package Level Fault Isolation Tools

As mentioned above EOS can damage the die as well as the package. Non-destructive package level fault isolation methods are often tried first to leave options for die level methods. Some of the most commonly used non-destructive tools for EOS fault isolation are optical examination, package level X-ray, acoustic microscopy and time domain reflectometry (TDR).

- **Optical Microscopy** – Simple planar microscopes, or binocular microscopes for three dimensional inspection, are very easy tools to use. When conducting any EOS analysis, it is good practice to use planar or three dimensional microscopy to detect any pin or package ball discoloration, which is evidence of high current flow. Package discoloration as well as changes in reflectivity of the molding compound can also indicate excessive heat generation and signs of EOS damage internal to the package. Lastly, passive components on the package such as resistors or capacitors should be inspected for signs of current induced Joule heating.

- **X-ray** - Since most components use high density materials for packaging interconnect, focused X-ray can be used for detecting displacement of packaging interconnect due to EOS as well as the physical presence of bond wires. This is particularly useful for "flip chip" packages where the lead or tin based C4 bumps are hidden between the die and the package. Focused X-ray will penetrate and effectively see through the package and die, but not the bumps. Since EOS often involves high currents and Joule heating, bumps that extrude or change size/density are typically associated with the failure. Any displaced bumps should be noted and cross mapped for further analysis. Bond wires should be continuous and provide electrical connection between die and package. EOS damage can melt and fuse bond wires.

- **Acoustic microscopy** is used to detect changes in the characteristics of the various laminar interfaces within a packaged component. The method uses a raster scanned ultrasonic transducer to project acoustic waves into a surface so that the reflection can be evaluated as a function of time and intensity in order to evaluate the depth and physical characteristics of discontinuities in the interfaces. The resulting raster scanned reflections paint a picture for a given depth of penetration. Since EOS-induced Joule heating can generate localized delamination, acoustic microscopy is another useful method for detecting EOS-damaged C4 bumps.

- **TDR** - Time domain reflectometry detects changes in the amplitude and reflected time of flight of electric pulses applied to the external connections on an IC package. Since EOS induced Joule heating can affect the morphology of a C4 bump, TDR can sometimes be used to determine if a bump has been affected by EOS. TDR can also detect if damage occurred in packaging interconnect or the die under certain circumstances. For wire bonded packages, TDR should be able to detect broken bond wires or defects in the die.

Once all non-destructive methods of evaluating the package have been attempted without success, it is appropriate to move to destructive but functionally conservative methods. This involves exposing the die surface and/or backside without damaging the bond wires. The goal is to expose the device for further evaluation without altering it parametrically or functionally. Acid etching is a proven method that is used to remove plastic packaging materials. Red and yellow fuming nitric acid are two of the more common etchants. There are two major drawbacks of using these materials. The first is the personnel hazard, so significant precautions should be used when applying these acids. The second is damage to the die by the acids. Modern processes and packages use copper interconnect. Copper is chemically reactive and can be easily damage by traditional etches. It is important to know what type of metallization is used on a die and in a package prior to using any chemical deprocessing methods. Manual methods for controlled applications can be used to selectively and controllably remove the plastic over the die until it is exposed. Commercially available pressure jet etchers can also be used to accomplish the same result quicker and more precisely, while minimizing some of the personnel hazards.

Once the die and bond-wires are exposed, the wires should be examined to determine if they have been stressed thermally, which would be an indication of EOS on that pin. An obvious example of being stressed thermally is when the wire is fused open. In addition, the die can be examined optically to determine if interconnect on the die surface shows signs of EOS. This is usually indicated by areas where the plastic package is difficult to remove. In these cases, the heat generated by an EOS event has caused further cross linking of the plastic, making it harder to remove. Exposure of the die while leaving bond wires intact also make it possible to perform the electrical fault isolation techniques discussed in the next section.

6.4.3.2 Electrical Fault Isolation Tools

Some of the most effective EOS fault isolation tools are the non-destructive electrical methods. They range in complexity from simple inexpensive tools such as current/voltage (I-V) curve tracers and liquid crystal to more complex tools such as infrared microscopy, optical emission microscopy, laser scanning microscopy (LSM), thermally induced voltage alteration (TIVA), XIVA (a trademarked technique similar to TIVA) and light-induced voltage alteration (LIVA), which are explained below.

a) **Passive I-V curve trace** - Since EOS frequently damages component pins and supplies, I-V curve trace is often one of the most useful tools for EOS diagnosis. Each pin or supply will have a voltage vs. current characteristic that is unique to that pin. It reflects the connection of all of the transistors, diodes, resistors, etc. on that pin and how they are tied to the other pins being curve traced. Changes in the junction and transistor leakage compared to good reference units are typical indicators of damage. Interpretation of the I-V curve trace requires an understanding of how the circuit should operate during the curve trace. Passive I-V analysis on signal pins should include traces to all pins including supplies, grounds, and other IO pins. An anomalous I-V trace highlights a conductive path not expected on a good unit or the loss of a desired signal or power trace; the latter state indicating a fused open electrical connection. These anomalous conductive paths are often the electrical source connections for biasing a damaged circuit. The following imaging methods can be used to further localize the defect site. It is important when performing passive I-V curve trace to limit the current and voltage excursion so as to not create, enhance or mask any original damage signature.

b) **Heat Detection and Microscopy** – Heat detection is a valuable tool for EOS analysis since EOS often involves damage that generates excess Joule heating. Two common methods are liquid crystal and infrared microscopy.

   i. **Liquid Crystal** – Liquid crystal has been used for decades as a low cost method for detecting heat generation in a die or package. Uniform layers of temperature sensitive liquid crystal are applied to a surface and polarized microscopes are then used to detect the heat induced transition of the crystal as a device is operated in a failing condition or test mode. The liquid crystal material comes in a number of transition temperatures with 29°C crystal being the most common. Higher temperature crystal can be used effectively for higher power shorts. Two of the challenges of liquid crystal are temperature control and resolution. The use of an external heat lamp can increase the sensitivity by raising the die temperature to just under the transition temperature of the crystal. In this case, the extra heat generated by the defect causes the crystal to transition. Alternatively, cooling of the die with compressed air can be used to temporarily transition the crystal back so

that the centroid of a heat source can be pinpointed as the defect re-heats. The spatial resolution limitation is limited by the optical microscope magnification used to image the crystal but is frequently not a problem for EOS FA due to the large areas that can be affected by EOS.

ii. **Infrared Microscopy** – Infrared microscopy is well suited to detecting localized regions of excess heat generation. It is often used on flip chip packaging, with some infrared detectors having the ability to see through silicon that is opaque to the human eye. Like liquid crystal, failing sites can be detected while operating or biased in a failing condition. Infrared microscopy also has resolution issues due to the long wavelength of infrared light. It can be longer than the circuits under analysis. But some infrared systems have the advantage of a large field of view, making them suitable for analysis of very large die where the analyst has minimal prior information on where to look for the EOS damage. Newer systems with lock-in capability offer higher sensitivities and better spatial resolution as well.

iii. **Emission Microscopy** – Emission Microscopy involves detection of higher frequency light than infrared microscopy, typically resulting from electron-hole recombination. Among other things, gate defects, saturated transistors, and forward biased junctions will generate light. Since transistors can generate light under normal conditions, the technique requires discrimination of damage induced light emissions from normal emissions. For failures exhibiting EOS damage, shorted transistors may stop emitting light, so discriminating a loss of light is also part of the analysis.

iv. **Laser Scanning Microscopy (LSM)** – LSM is another valuable tool for EOS detection. The method uses an incident laser beam at laser frequencies that are transparent to many types of silicon. This makes them particularly useful for imaging flip chip devices. Images are created by raster scanning a surface with the incident beam and detecting the reflected light. Since the dopants used in transistor fabrication alter the transmissivity of silicon, doped regions will have different shading and contrast. This allows them to show up as distinct structures that can be used for navigating to areas of interest when compared to the transistor layout. Joule heating can also alter the transmissivity of the silicon, allowing the LSM to sometimes see overheated or heat damaged circuits. This makes simple LSM imaging a potentially powerful tool for EOS damaged flip chip devices due to the localized Joule heating frequently generated during EOS events.

c) OBIRCH/TIVA/XIVA

If the incident LSM laser beam has a frequency in the 1340 nm range, which generates thermal heating in silicon, an LSM can both view and heat the silicon. This is because localized laser heating can also selectively alter the conductivity of small ohmic shorts on a die. This conductivity alteration can be exploited for failure analysis.

LSM based fault isolation systems typically include a power supply with constant current and/or constant voltage capability. The supply provides the ability to detect fluctuations in voltage or current to a failing die circuit while the LSM simultaneously raster scans the die surface with the incident laser beam to alter the resistance of the failing circuit. The position of the beam is known by the system, making it possible for the system to generate an electrical response map that can be superimposed over the LSM image.

Superimposing electrical response images over LSM images results in methods called OBIRCH (optical beam induced resistance change), TIVA (thermally induced voltage alteration) or XIVA (a trademarked technique similar to TIVA). These are good methods for EOS analysis; often providing physical maps of the location of micro-shorts. In order to avoid pursuing false sites, bias voltages should be chosen carefully and any sites that are found should be considered for their potential to alter the circuit. Diode and transistor threshold voltages are very important considerations as is the enhanced temperature sensitivity of some circuit components in specific bias condition ranges.

6.4.4 Physical Failure Analysis Methods and Techniques

Once a suspect area of failure has been identified through fault isolation, it is typical to perform physical analysis to validate the location and examine the extent of damage. Physical analysis can be a very time consuming process requiring specialized tools. Performing physical analysis requires experience with these specialized tools as well as knowledge of silicon and package fabrication techniques. This section will discuss some of the techniques used and how they apply to EOS analysis.

a) **Package Level Physical Analysis –** Failures exhibiting EOS damage typically do not damage packaging materials because most packages are electromechanically more robust than the die. That said, some packages are less robust than others, and sustained electrical operation after damage has occurred can cause Joule heating and collateral symptoms of failure in the package. As a consequence, package level physical analysis is sometimes needed for failures exhibiting EOS damage. Any package damage symptoms should be noted and correlated to circuitry in the die when they are observed. Aside from the non-destructive methods discussed previously in this chapter, destructive methods range from mechanical cross sections of the package and/or die to simple die removal and package surface inspection. Removal of the die is also often needed to perform die level physical analysis, which is discussed next.

b) **Die Level Physical Analysis –** Die level analysis on failures exhibiting EOS damage is a process which begins by applying all available test and fault isolation information to target specific areas on the die for visualization to 1) validate that the areas is damaged by EOS and 2) determine the extent of damage. A number of methods and types of equipment are available to accomplish these goals; each providing varying degrees of visual resolution and physical composition information. For most of these techniques, the first step is to prepare the die for analysis.

   i) **Die Sample preparation –** A finished silicon die typically consists of a thick layer of silicon that provides structural support for extremely thin films of ion implanted silicon, polysilicon, metallization and dielectric. Determining the extent of damage in these films can provide clues to the root cause. To characterize this damage, a 3 dimensional approach is needed. This can be accomplished by meticulously delayering and inspecting each layer (i.e., planar) or alternatively cutting through the stack of layers to target a specific x-y location within the stack (i.e., cross sectional).

      - **Planar sample preparation** for EOS involves removal of normal or undamaged layers to expose the damaged layer(s) at the x-y location of interest. There are two basic approaches to physically deprocessing a die; front side and back side.

- **Back side deprocessing** is a method, typically applicable to flip chip die, that uses chemical or ion etching to essentially remove the majority of the thick silicon to get as close as possible to the thin films without damaging them. The advantage of back side deprocessing is that if done properly, it results in uniform exposure of the implanted transistor films from the underside. The disadvantage of back side viewing is that some types of transistor level EOS damage may not be seen from the backside, and it is not conducive to examination of the films above the transistors. As a consequence, additional deprocessing may be required.

- **Front side deprocessing** uses chemical, ion or mechanical methods to selectively remove one or more of the thin films, starting at the top layer (typically the bonding layer). After removing a layer, the area of interest is inspected to ensure that the desired amount of material was removed at each step. Methods of inspection will be discussed later.

Various chemical and ion etch recipes can be used, with many of the etchants being toxic or corrosive. In addition, both ion and chemical etch recipes must be precisely timed and controlled to avoid over or under etching. Given the assortment of recipes available, these will not be discussed in much detail.

Mechanical polish is an alternative method that is preferred by some analysts. This method uses films or slurries to slowly and controllably remove a layer by polishing away the material in a given layer until the desired depth is achieved at the location of interest. Mechanical polish must also be precisely controlled to avoid excessive removal of a given layer. Mechanical polish can also cause uneven material removal, with the outer edges polishing away faster than the center. This means that some skill and practice is needed to ensure that any area of interest gets properly exposed. The repeated inspection process after layer removal can also be quite tedious. The advantage of mechanical polish is that it is not toxic or corrosive, and it can be fairly well controlled with practice.

- **Cross Sectional Analysis Sample Preparation –** While top down inspection of an area of interest will often provide all needed information, EOS damage can affect multiple layers. Determining the extent of damage is often critical for determining root cause and cross sections can sometimes be the most effective and least time consuming approach.

  - **Mechanical saw/polish** is one method for performing a cross section. But it can be quite imprecise and an area of interest can be easily missed if the analyst is not cautious and meticulous. Like mechanical delayering, repeated inspections are often needed in order to polish into the three dimensional area of interest.

  - **Focused Ion Beam (FIB) Milling** is a method preferred by many analysts for cross sections if it is available. These systems typically have some sort of imaging system such as an electron or ion based microscope that facilitates navigation to an area of interest and allows the analyst to view the progress of the milling. Unlike mechanical

cross section, FIB is an in-situ process with typically higher magnification, making it much more precise and controllable.

c. Imaging and elemental analysis – Once an EOS damage area of interest has been prepared through delayering, cross sectional analysis or, in some cases, no preparation at all, high magnification imaging and sometimes elemental analysis are typically performed. The sophistication of the tools ranges from simple optical and basic electron microscopes to more sophisticated tools like laser scanning microscopes and transmission electron microscopes. These are described below.

i) Optical Microscopy – Although planar and three dimensional optical as well as laser scanning microscopy are discussed in the package and electrical fault isolation sections, they can also be used for physical analysis. During both delayering and mechanical cross sections, microscopy is often preferred over laser scanning microscopy for ease of use. Unlike electron microscopy, optical microscopy also provides color images, which can be useful in detecting electrically stressed circuits since Joule heating can discolor both die and package materials. Extreme Joule heating can also affect silicon dopants, which affects the emissivity of the silicon during laser scanning microscopy and can be a sign of EOS.

ii) **Electron Microscopy –** To acquire images of features on a die that are smaller than the wavelength of optical light, electron microscopy is typically used. The basic types of electron microscopes and their usage on failures exhibiting EOS damage are described below.

- **Scanning Electron Microscopy (SEM)** uses a raster scanned incident electron beam to irradiate a surface while an electromagnetic lens is used to focus and classify the energy of the secondary and backscattered electrons resulting from the incident beam to create the SEM image. Electron backscatter and secondary electron generation are both affected by the atomic mass and density of the materials in the image field, which means that information about the composition of the materials comprising an SEM scanning field can be obtained. This allows silicon to be discriminated from metals and metal infused silicon. In addition to the energy information, the angle of incidence of the electron beam with respect to the surface can be adjusted to create three dimensional effects.

  Some SEM systems also have the capability to do energy dispersive X-ray (EDX) to perform elemental analysis of the materials on a surface. As the electron beam displaces electrons from the valence bands of the materials being irradiated, x-rays are produced having energies unique to the material being analyzed. Classifying and correlating these energies with an energy versus element look up table leads to identification of the elements. While this can be done manually, many systems have the capability to do this automatically. Many systems can also produce spatial vs. elemental images that are extremely useful in some cases.

  Since high current EOS can displace metals with Joule heating, EOS damage is often obvious. If needed, areas of suspected EOS damage can be compared to reference

images from an undamaged unit or identical area on the damaged unit to determine if the damage is real. Low current but high voltage EOS may not create the Joule heating necessary to displace metals.

EOS damage can also occur in a gate oxide, which is an extremely thin layer. Magnifications higher than the capability of an SEM may be needed. In such cases, transmission electron microscopy may be the only alternative.

- **Transmission Electron Microscopy (TEM) –** Like SEM, TEM relies on electrons and electromagnetic lenses for imaging. However, unlike SEM which detects electrons coming from a surface, TEM shoots the electron beam though an extremely thin slice of the silicon. In addition, TEM only produces two dimensional images. However, newer generations of TEMs have much better resolution than the SEM. The resolution is good enough to see atomic and molecular arrays in thin films. This can prove useful when detecting EOS induced gate oxide damage. Like the SEM, the TEM can also do elemental analysis and mapping; but at higher resolution.

  Although the resolution of TEM is superior to SEM, sample preparation is not. While samples can be prepared through polish, there is a relatively high probability of missing a very small area of interest. The most practical approach is often to use a FIB mill. Samples can be both planar and cross sectional. In addition, unlike SEM, information is gained on the entire slice of material and not just the surface. This thickness should be taken into consideration when interpreting the results of any TEM analysis.

d. Picoprobing and Microprobing – There are times when damage to a sub circuit of a device may be suspected, but no evidence is seen by imaging analysis. If electrical access points to the circuit of interest reside within the thin film stack, it may be necessary to physically probe the access points to provide electrical contact.

Specialized probers are available to do this. Usually combined with optical and in some cases electron microscopy, multiple probes can be placed to drive signals and measure the response of the circuit. Probing can measure the resistance of circuits to confirm damage. It can also generate transistor and diode IV curves to detect damage such as leakage or to determine circuit characteristics such as thresholds and saturation current, which can be indications of gate oxide stress or damage mechanisms that will be discussed later in this chapter.

6.5 Analysis of Damage Mechanisms for EOS

Component damage due to EOS can manifest itself many different ways. The total energy of a non-complex single EOS pulse is defined by the equation Energy (J) = Voltage (V) * Current (A) * time (seconds). This means that the degree of damage is a strong function of the power (i.e., voltage multiplied by current) and duration of the event that caused the damage; with circuit and device construction being other factors. EIPD symptoms can range from gate oxide damage in one leg of a transistor to substantial movement of the conductive metal films in the vicinity of a damage site. Secondary damage, unrelated to the original cause of failure, can also be induced if system malfunction is catastrophic and sustained after the initial failure occurs. This makes understanding

the mechanisms that cause both EOS damage and secondary symptoms critically important to determining a cause for the damage.

6.5.1 Voltage and Current Effects as a Function of Time

The three critical factors that control EOS sensitivity are voltage, current and time. Sensitivity to these factors is dependent on the specific process technology used to manufacture a device as well as the design of the device. Other effects include the temperature of the device at the time the EOS event occurred. Understanding these effects is critical to determining possible root causes. How these factors can affect EOS sensitivity and how they interact with each other are described in this section.

6.5.1.1 Voltage as a Function of Time

The effects of voltage and time are well known to engineers involved in device reliability. A classic example of the effect is illustrated by high temperature operating life (HTOL) stress. Reliability engineers must simulate the lifetime of a device in a compressed period of time to guarantee the device will survive a lifetime at normal conditions. This is typically accomplished by subjecting a statistical population of devices to elevated voltage and elevated temperature operation. Theoretical and empirically derived equations are then used to model the device aging and calculate the predicted device lifetime.

a) **Gate Oxide -** Elevated voltage can significantly affect transistor gate oxides, with the impact being exponentially dependent on time. Voltage slightly above nominal can take days to months to produce noticeable effects, while extremely high voltages can produce effects in fractions of a second. Some of the mechanisms resulting from elevated voltage stress on gate oxide are hot carrier injection (HCI), time dependent dielectric breakdown (TDDB) and biased temperature instability (BTI).

   i) **HCI** occurs as a result of high energy carriers in the channel. This can occur from transistors switching operating states, such as in logic devices, and also can occur in analog circuits under DC operating conditions. There are several types of HCI whose description is beyond the scope of this paper, but the net effect of all of them is that carriers (i.e., electrons or holes) are injected into the gate oxide. The net result is transistor degradation. This transistor degradation can degrade the operating window of the device. If severe enough, the device will not function at any voltage or frequency. Detecting the presence of HCI can be challenging from an FA imaging perspective, but it can be detected through parametric analysis of a suspect transistor with tools like microprobing.

   ii) **TDDB** occurs when gate oxide traps are generated in the gate oxide and line up to form a channel that conducts and self-propagates to failure. There is some debate on the exact mechanism that causes TDDB, but it is strongly dependent on elevated voltage. Like HCI, TDDB also causes device degradation since the string of oxide traps that form across the oxide will conduct and make the gate leaky. This would tend to affect the drive strengths and threshold of the transistor. Like HCI, TDDB can be detected by microprobing.

   iii) **BTI** is a DC stress mechanism that also affects the gate oxide. It is accelerated by both voltage and temperature. Gate Oxide trap generation is believed to account for the

negative biased temperature instability (NBTI) effect, although there can be several sources for the traps. BTI is a device degradation mechanism like HCI and TDDB, however it can partially recover within a short period of time. Unfortunately, the recovery is only temporary, and will quickly re-induce once it occurs in a circuit. Probing of a BTI affected circuit will show transistor threshold and drive strength degradation.

If probing shows a significant increase in gate to drain or source leakage, that could be an indication of gate oxide rupture. Oxide rupture occurs when the voltage across the gate is high enough to punch through the weakest spot in the oxide layer due to loss of electrical isolation. While TDDB creates oxide trap weak spots that form with bias and time, rupture can occur at thin spots or discontinuities in the oxide. The result is a hole that can self-propagate from Joule heating as current flows through the hole. Probing and physical examination of the oxide (sometimes requiring stains) can reveal evidence of oxide rupture.

b) Interlevel Dielectric Breakdown – Semiconductor film stacks use dielectric materials to insulate the electrically conductive layers and traces within the films. A low dielectric constant is desired to reduce the capacitive coupling between the conductors. If the voltage potential between two isolated conductors gets high enough, the dielectric can break down and cause an electrical conduction path between the conductors. If enough Joule heating occurs at the point of breakdown, the point can self propagate to the point that conductors such as copper or aluminum migrate or extrude into the point of breakdown. Once conductor to conductor contact is established, the current will increase with little opposition resulting in a runaway situation. The net effect is to cause additional damage symptoms.

c) Junction Conduction – The most common form of EOS occurs when a junction conducts too much current, causing melting of the silicon and/or damage to the interconnect tied to the junction. The P-N junction is the most basic semiconductor junction, forming a circuit element which conducts current when exposed to one voltage polarity but blocks current when the voltage polarity is reversed. These operational modes are termed forward bias and reverse bias, respectively. In the forward bias mode the p-type anode is positive in voltage compared to the N-type cathode, and there is current conduction once the bias across the junction exceeds a critical voltage threshold. This voltage is also the forward voltage drop. Each type of diode has a unique forward voltage drop ranging from a few tenths of a volt to about a volt. P-N junctions are the most common diodes found in integrated circuits. They are also fundamental elements of bipolar junction transistors (BJTs), and MOSFETS.

In reverse bias the diode is blocking current flow and negative anode to cathode voltage is applied. The key difference is that there is an inherent limit on the magnitude of reverse bias that the diode can handle. This limit is based on its construction and can range from a few volts to thousands of volts.

i. **Forward bias diode damage** – A forward bias diode has a low forward voltage drop and the current is spread throughout the 3-dimensional P-N junction interface surfaces within the volume of the diode. This provides the most robust conduction behavior available. The power dissipation (P = I*V) is low and the total dissipation of the P-N junction surface area is high. Under EOS level stress conditions though, the metal

interconnect may not provide a uniform conduction path. Due to the high currents typically resulting from the forward biased diode, voltage drops in the metal can focus more of the current into localized areas of the diode, causing higher current densities and power dissipation. If too much current flows for too long, Joule heating damage can occur. The damage can be in the form of interconnect melting, interconnect diffusing into the diode itself through the contacts, and disruptions in the diffusion making up the diode due to high temperature and high current. The damage pattern for a forward bias, uniformly connected diode will show damage uniformly across the body of the diode. Localization of the damage could indicate a metal connection current choke point or a different mechanism than forward bias damage.

ii. **Reverse Bias Diode Breakdown** – In contrast to the forward biased diode, a reverse biased diode in breakdown has the least robust conduction mechanism. The voltage dropped across the reverse bias diode is found in the depletion regions near the metallurgical junction, the surface at which the doping changes from P to N type. This is a very small volume in the diode. When conduction does start to occur, the voltage drop, current density and consequently the power dissipation is very high. High power dissipation and small dissipation volume leads to very poor physical robustness. This is compounded by localized breakdown in the diode due to random process defects and layout effects, further localizing the power dissipation. Small junctions taken into breakdown are extremely weak and are easily damaged by EOS. (The value of reverse bias diode breakdown voltage for the diodes in a technology is a major component in determining the SOA and AMR of integrated circuit technologies.)

iii. **Junction Proximity Effects** – Semiconductor circuits consist of many devices connected in a manner to perform a function in the least amount of space. One side effect of placing many circuit elements closely packed together is the formation of parasitic transistor elements. The most damaging can be parasitic NPN and positive-negative-positive (PNP) transistors. Parasitic NPN can be formed from antenna diodes in close proximity to a MOS transistor or even from two diffused N-type resistors. The NPN transistor has an operational characteristic defined as snap-back, which can cause significant damage if it is activated. Snap-back is a mode of breakdown where the voltage across the collector/emitter drops significantly and the current increases after reaching the snapback voltage threshold for the transistor. This negative differential resistance effect can intensify the current flow in the transistor, causing physical damage to the transistor. If a parasitic NPN is triggered into snap-back, it will typically short out and cause circuit failure. Diode forward conduction or breakdown is an example of an initiating event for this snap-back behavior.

In the case where an NPN and PNP transistor are closely spaced together there is a potential to form a parasitic silicon controlled rectifier (SCR). A sustained activation of this parasitic SCR is commonly referred to as latch-up. All bulk CMOS circuits contain parasitic SCRs, and there are well known methods for designing circuits to be resistant to their formation. These can be triggered from a blocking state (non-conducting) to a conducting state by external events such as supply transients, current injection on IO lines or ESD, as well as internal transient events such as the forward bias or breakdown of a diode junction. Once the SCR is triggered, it will go to its low holding voltage, high current state, effectively shorting out the supplies. Damage seen

from this behavior is melted metal lines as well as melted silicon in the area where the SCR triggered. SCR damage should be considered as a possibility when physical damage in the silicon is seen between a P region in an N-well and an N region in a P-well since this is the main current path during latch-up.

6.5.1.2 Current as a Function of Time

While voltage induced by EOS can cause gate or interlevel dielectric breakdown, excessive current flow induced by EOS can cause enough Joule heating to result in failure of a circuit. Excessive Joule heating can also increase sensitivity to some of the voltage vs. time effects discussed above.

Current stress is typically the result of some sort of malfunction of the system. Potential causes include signal pin contention due to a loss of sync between components, inductive transients due to sudden interruption of current flow, and inductor capacitor (LC) transients from hot plug, board capacitance, and cable inductance, to name a few.

The high current flow can be the result of elevated voltage applied to a low resistance path that was not intended to be exposed to the elevated voltage. It can also be caused when another component on a board fails, shorting high voltage to a low voltage pin. Excessive Joule heating in a metal conductor can cause expansion of the metal. If the expansion is excessive, the mechanical effects on the thin films can lead to failure as discussed next.

a) **Diffusion Barrier Rupture** – Metal conductors such as copper have thin barriers that mechanically encase the metal and physically isolate the conductor from the dielectric. Copper tends to be plastic and capable of extruding under pressure. The plasticity increases with temperature. Barrier metals have higher melting points and greater hardness than copper and they provide the mechanical barrier. Since copper can also migrate into the space between dielectric molecules, the barrier (which doesn't migrate) forms a physical barrier between the two.

   Current induced Joule heating will cause the metal to expand as mentioned previously, which increases the internal pressure seen on the barrier metal. If the barrier cracks due to the pressure, the copper can extrude and/or migrate through the crack and into the dielectric. Eventually, a conductive bridge forms with adjacent conductor lines. Once this occurs, runaway and catastrophic failure can occur. It should also be noted that low-K dielectrics have inherently lower mechanical strength and are easier to damage when subjected to thermal/mechanical stress.

b) **Metal Damage –** Electrical bias induced Joule heating in metal lines, vias and contacts can cause interesting effects. Temperatures can get high enough to cause the metals to physically transition to a plastic or molten state. In this state, copper can literally flow from one point in a metal line to another, compressing low-K dielectrics as metal collects in one area and drains metal from another. This can cause secondary shorts and mechanical damage within the thin films. If the current flow is high enough, metal "burnout" can occur at current constrictions and the line, via, or contact will become highly resistive at that location. This makes electrical opens at a pin a possible symptom of failure.

c) **Joule heating induced diffusion** – The Joule heating created by EOS current flow can create surprisingly high temperatures. The temperature can be high enough to diffuse transistor

dopants and polysilicide layers, which can often be observed with optical, laser scanning and electron microscopy. Both types of diffusion can adversely affect transistors and diodes to the point of device failure. Observation of these effects in specific circuit elements and correlation of the effects to circuit schematics can be quite useful in determining root cause of an EOS damage.

6.6 Overstress Power vs. Time

Having described some of the voltage and current effects as a function of time, it should be noted that there are several generations of mathematical models available for determining the ability of a circuit to tolerate electrical self-heating power as a function of time. Two of the better known models were developed by Wunsch-Bell and Dwyer-Franklin-Campbell. These models are based on the power injected into and the rate of heat transfer away from the affected circuit(s). If the heat transfer rate away from the heated circuit is too slow, temperatures can rapidly rise to produce the symptoms described in Section 6.5.1.2.

Wunsch-Bell assumed a planar geometry, uniform thermal conductivity and one dimensional heat flow [1]. Dwyer-Franklin-Campbell later developed a physical model of a parallel-piped for three dimensional heat flow [2, 3]. The basic shape of the curves are driven by the amplitude of the power injected into a circuit, the duration of the power injection and heat transfer capability of the circuit along with the materials that surround it. Destruction is presumed to take place at a specific threshold temperature, generated on the surface at the uniform, constant heat source. The models are capable of generating curves for power pulse duration on the X-axis and pulse amplitude on the Y-axis. The area below the curve is considered the safe operating region. If the amplitude and/or duration of a power pulse is above the curve boundary, the circuit will fail (aka, the "power to failure" boundary). Both models generate curves that show the power threshold to failure decreasing asymptotically as the amount of time stress is applied increases. Most literature summarizing the two models define 4 basic regions, an example of which is shown in Figure 83 [4]. In this plot, P_f is defined as power to failure, t_f is defined as time to failure and Q is the rate of heat transfer through conduction.

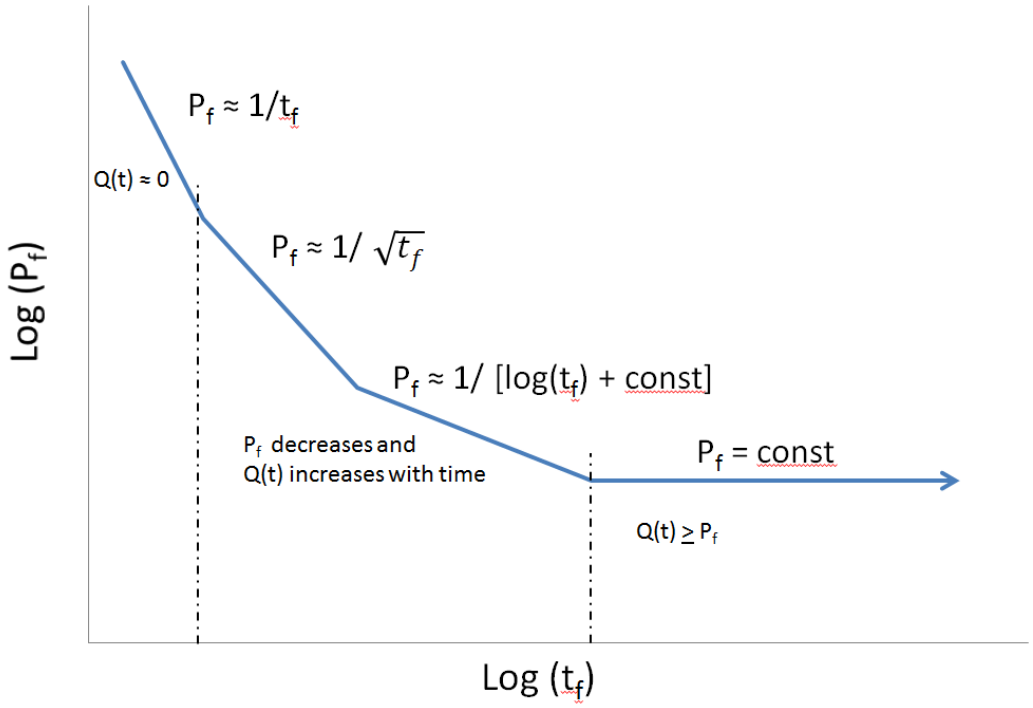


Figure 83: Example Power to Failure Curve

- The left edge of the curve starts with very short duration high power pulses. The pulses are so short that essentially no heat transfer to the surrounding metal and silicon occurs during the pulse. Pulses of this duration are considered adiabatic, and can cause circuit failure if the temperature resulting from the pulse exceeds the critical failure temperature of at least one of the circuit components. The power to failure (P_f) for this regions is defined by the expression $P_f \approx 1/t_f$, for which t_f is the time to failure, and corresponds to heating of the heat-generating element (e.g., metal) to a critical temperature as determined by its heat capacity.

- As the pulse amplitude drops, the amount of heat injected as a function of time drops and the circuit can tolerate longer pulses. Heat transfer to the surrounding bulk material starts to occur during the pulse, which extends the amount of time the circuit can withstand a pulse. As a consequence, the slope transitions into a region defined by $P_f \approx 1/\text{sqrt}(t_f)$, and then into a region defined by $P_f \approx 1/[\log(t_f) + \text{constant}]$.

- If injected power drops low enough, the curve flattens and a steady state region is reached where the heat transfer rate away from the circuit equals the applied power. The steady state region is therefore defined by $P_f \approx$ constant.

Recently, a new power to failure model has been developed that extends the Wunsch-Bell approximation to account for heat flow more accurately. The model exploits the fact that the differential equations used for basic transmission line modeling have the same form as a one dimensional heat flow equation. The Wunsch-Bell approximation thus results from an infinite transmission line, while the full Dwyer curve results when the line is terminated by a resistor or short (i.e., heat sink). A capacitor in front of the line then represents the heat capacity of the heat

source for the adiabatic (1/t) section. The Wunsch-Bell portion ($1/\sqrt{t}$) of such a curve then emerges as a time region between adiabatic and long-term uniform heat flow. A detailed summary of the model, how it was derived, and conclusions from the model are found in Appendix B.

6.7 Final Diagnosis of the Cause and Conclusion

This chapter has focused on the methodology for isolating the location of EOS damage and gathering as much information about the physical properties of the damage site as well as failure mechanisms that result from EOS damage. However, the end goal of any EOS failure analysis project is to determine cause. Not only does the physical event that caused damage, such as DC overvoltage, voltage transients or system ESD, need to be understood, the cause of the physical mechanism needs to be understood as well. Symptoms suggesting conditions like DC overvoltage on a signal pin may be relatively easy to isolate and identify. The greater challenge may be determining why the DC overvoltage occurred in the first place and this requires close cooperation between the supplier and customer to address.

6.7.1 Forensic Failure Analysis

Assuming that FA has isolated damage in a component to a sub function of interest and provided physical information on the electrical nature of the event, determining the cause often requires an expansion of the investigation beyond the failure analysis lab. It is often necessary to perceive the failing sub function of the failing component in the system as a complete circuit whose operation must be understood while in the condition that failure analysis suggests it was subjected to.

As an example, damage to an ESD diode residing between an IO pin and a voltage supply rail for that pin could be due to EOS by ESD or EOS unrelated to ESD. Uniform heating symptoms in the diode could indicate a sustained forward overcurrent due to a DC or long transient overvoltage event. An isolated damage site could be an indication of a short duration overcurrent event such as reverse bias diode breakdown due to component or board level ESD. Analyzing the polarity and time vs. energy characteristics of the damaging event is often the first step in isolating root cause. The next step is to look at the failing circuit as a whole and determine how this event was applied to the circuit in the first place

The information described in the high level preparation and documentation sections of this chapter often prove useful when a failing circuit has been identified along with the electrical mechanism that caused the damage. Examples of how this information can be applied are shown below.

- For EOS events like forward overcurrent in an ESD diode, system schematics can be reviewed to determine if malfunction of another system component (passive or active) could account for the failure.
- System operating conditions can be scrutinized to ensure they meet datasheet requirements for the damaged component.
- Board components connected to the failing sub circuit can be researched to ensure they are compliant with all of the requirements specified in the manufacturing datasheet.
- External components connected to the system at the time of failure can be electrically analyzed to ensure they do not generate events that exceed absolute maximum ratings when operated or plugged in.

- If system ESD is suspected, system protective components such as external overvoltage shunts can be researched to ensure they are properly used and have adequate response times and protective capability.
- If component ESD is suspected, factory ESD levels could be scrutinized to ensure they are compliant with industry specifications.

6.7.2 System Electrical Analysis

Sometimes, the FA result and the available "post mortem" analysis information on the nature of the failure are insufficient to determine a cause. In addition, some failures exhibiting EOS damage can be excessively damaged by collateral damage due to electrical operation after the overstress event. However, knowing what sub-function of a component is damaged can be useful if the failing system or a functionally equivalent system is available for electrical analysis.

Electrical analysis of a failing system after replacing a damaged component may be the last resort in helping determine a root cause. High speed oscilloscopes generally provide the best results. The key is to analyze any suspect signals using a mode that replicates what the damaged component saw at the time of failure as closely as possible. A worst case event may not be seen during the analysis, but the presence of any potential stress event should be investigated due to the possibility that a more severe version will be seen in a small percentage of systems. Methods for accomplishing this include the following:

- Use of differential probes with probe tips positioned as close as possible to the pin(s) of interest. Differential probes eliminate common mode noise while close positioning of the probe tips minimizes the effect of signal trace parasitics on the fidelity of the monitored signal.

- Duplicate the operational conditions that induced failure during the electrical analysis while monitoring with a time base appropriate for the speed of the event. As an example, if a failure occurs when a cable or external component is plugged into a system, suspect pins should be electrically analyzed while the offending cable/component is plugged in using an oscilloscope time base that ensures any extremely high speed events are captured if they exist.

- Set elevated oscilloscope voltage triggers to capture any overvoltage event while avoiding or discriminating the capture of normal events. This usually involves viewing the peak amplitude of the signal in normal operation, and then setting the trigger slightly above that level.

- Set software triggers when the event is observed to occur during execution of a specific function or instruction.

6.7.3 Failure Analysis Signature Matching

The concept of creating a failure signature with a specific type of stress to match the failure signature of a device as proof of possible root causes is a fairly common idea. Examples would be to intentionally ESD zap a unit to failure and then perform failure analysis to see what type of damage was induced. Another example of this approach would be to increase supply voltage or inject supply over-voltage transients until a device fails. Subsequent FA could form the basis for signature matching.

The theory is that if a characteristic failure "signature" by an event such as DC overvoltage can be matched to EOS damage, then DC overvoltage must be the cause. In fact, this can be a misleading approach. As noted by Smedes, Christoforou and Zhao [5], varying stress amplitude and duration can produce similar failure symptoms. A voltage transient of higher amplitude and shorter duration could produce a similar characteristic signature but have a different EIPD location. That said, matching a field failure signature with a known stress event can add confidence to conclusions based on forensic analysis of the silicon and/or electrical analysis of the system. So this approach can be useful under the proper circumstances.

6.7.4 Time Required for EOS Failure Analysis and Diagnosis

When a device is submitted for analysis of suspected EOS damage, the typical follow up question is: How long will it take to complete the analysis? This can be a difficult question to answer since a number of different variables can impact both the time required for analysis and the probability of success. Failure analysis times can range from days to months. The factors that play a critical role in the time to complete a successful analysis include the following:

- The quality of the descriptive information provided by the requestor when the device was submitted for analysis. A thorough description of the device history and symptoms of the damage, as described in Section 6.1. This can speed analysis if the analyst does not have to gather data that was collected by the requestor before submission; while also insuring the analyst is focusing on the symptoms of greatest interest to the requestor.

- The degree of damage the device sustained during the EOS event. Severe collateral damage can create secondary symptoms that are difficult to differentiate from the true cause of damage. If power and signal delivery capability are compromised, electrical fault isolation may also not be possible, which will impede completion time of the analysis as well as the probability of determining the cause of damage.

- Electrical characterization, fault isolation capability and physical analysis tool capability of the lab. Availability of the tools described in Section 6.4 can be a factor in the time required for analysis since some tools can complete a certain type of analysis faster or more accurately than others.

- Analytical personnel capability. Many of the tools in Section 6.4 require highly trained and experienced personnel to be effective. More experienced personnel will typically complete an analysis faster and more accurately than less experienced personnel. Labs that use a team approach that bring together tool specialists require a good coordinator to optimize the effectiveness of the team.

- The failure mechanism itself. Some failure mechanisms can take longer to identify than others. The usefulness of characterization data and fault isolation tools can vary with the degree and type of damage. In addition, some types of physical analysis, such as low level gate oxide damage, can take longer than other failure mechanisms (e.g., upper level metal damage). Some mechanisms may lead to additional follow up analysis, an example being suspected interconnect damage that turns out to be caused by a mechanism in the active silicon such as a damaged transistor channel; or require analysis of a second unit to confirm.

- Product complexity. A more complex device typically requires much more complex ATE diagnostic tools in order to better isolate the failing circuit block. In addition, very high resolution electrical fault isolation tools are typically required for the latest technologies prior to physical failure analysis. This complexity can add time to the fault isolation process**,** but is critical to complete before physical failure analysis starts in order to ensure a higher degree of success in finding the cause of the damage.

References

[1] D.C. Wunsch and R.R. Bell, "Determination of Threshold Failure Levels of Semiconductor Diodes and Transistors due to Pulse Voltages," IEEE Trans. Nuc. Sci., NS-15, pp. 244-259, 1968.

[2] V. M. Dwyer, A. J. Franklin, and D. S. Campbell, "Thermal Failure in Semiconductor Devices", Solid State Electronics, vol. 33. pp. 553-560, 1990.

[3] V. M. Dwyer, A. J. Franklin, and D. S. Campbell, "Electrostatic Discharge Thermal Failure in Semiconductor Devices", IEEE Trans. Elec. Dev., vol. 37, no. 11, pp. 2381-87, Nov. 1990.

[4] C. Diaz, C. Duvvury, S.M. Kang, "Thermal Failure Simulation for Electrical Overstress in Semiconductor Devices", Proceedings of the International Symposium on Circuits and Systems, 1993, pp. 1389-1392, vol. 2.

[5] T. Smedes, Y Christoforou, S. Zhao, "Characterization Methods to replicate EOS Fails", Proceedings of the Electrical Overstress / Electrostatic Discharge Symposium, 2014, paper 9A.3

Chapter 7: Minimization and Mitigation of EOS

Charvaka Duvvury, Texas Instruments (Retired)
Reinhold Gärtner, Infineon
John Kinnear, IBM
Hans Kunz, Texas Instruments
Alan Righter, Analog Devices
Christoph Thienel, Bosch

7.0 Introduction

The purpose of this chapter is to review possible strategies to eliminate many avoidable cases of EOS damage that might occur during the life of an IC from the initial design phase to final system implementation and field operation. This chapter will address every aspect, from the impact of technology scaling, advanced ESD design practices, product testing environment through the field reliability impact. This chapter will also include the lessons from the previous chapters.

7.1 Lessons Learned to Minimize EOS Damage

This section will describe some typical experiences from various fields which are shown here as a demonstration of ways to help improve EOS understanding and minimize EOS damage.

7.1.1 Lessons from IC Design Issues

There are examples of IC design issues which have resulted in failures exhibiting EOS damage. Chapter 5 gives an example of EOS damage during a 6 V burn-in. The ASIC used a rail clamp NMOS on its VDDA supply which had a bipolar holding voltage below 6 V. Noise spikes on the burn-in supply caused triggering of the NMOS and the device remained in snapback mode, which carried current for an extended time, resulting in damage. The cause of the damage was a high resistance grounded P-well connection that enhanced the ability of the rail clamp device to snapback. The fix was to reduce the resistance and connection of the ground rail to the P-well backgate. A lesson learned in this example is to ensure that burn-in supplies have good noise control and that the on-chip supply protection has a trigger voltage above expected supply transient values while also avoiding a holding voltage below the burn-in supply voltage.

In another example involved VDD pin damage during burn-in life tests. The ESD device trigger voltage was very close and just above the burn-in voltage level. The ESD device was a substrate triggered NMOS device designed to meet 4 kV HBM as required by the customer. After discussions with the customer that these failures came from the aggressive ESD protection device, the guard ring spacing of the protection device was modified to increase its trigger voltage at the expense of the 4 kV HBM requirement. The new device still had solid HBM performance, but the EOS damage during burn-in was eliminated.

7.1.2 Lessons from Factory Floor Issues

One of the major contributors to EOS in the electronic factories is poor grounding. A good example is a case which occurred at a semiconductor packaging facility. The production lots experienced very low yields, close to 0 %, for power MOSFET devices in TO-220 packages. The packages came from different technologies, different wafer lots and even different wafer fabrication sites. During physical failure analysis all devices showed a hot spot due to EIPD (see Figure 84).

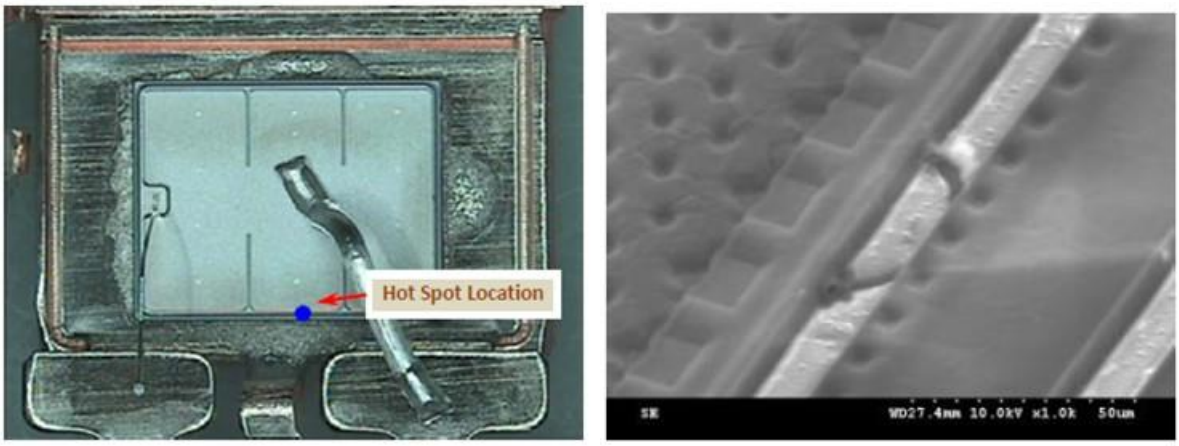


Figure 84: Hot Spot on Failing Device (left) and Corresponding SEM Picture (right)

The evaluation showed that the failures were generated in the aluminum wire bonding process. However, it was difficult to identify which part of the wire bonding process went wrong and was causing the damage. Normal grounding checks showed no evidence of poor grounding. Unfortunately, the grounding of the moving part of the bonding machine (metallic bond head) was not checked because the specification was not available. Regular resistance measurements showed big variations when the equipment was powered, and personnel could not decide what reading was good or bad. Therefore, an alternative AC voltage check was applied to verify the grounding conditions of the wire bonders using a digital multi-meter. With this alternative check it was found that the ground connection of the wire clamper, which was only grounded via bearings, was not good enough. As the grounding through the bearings deteriorated over time, an AC voltage was induced on the bond head and transferred directly to the bond pad during wire bonding which resulted in electrically induced EOS damage. Once the grounding issue was fixed, no more EOS damage was detected. More details on this and other examples can be found in [1, 2]. The example above shows that grounding can deteriorate over time, especially on the moving parts of automated handling equipment and therefore needs to be regularly checked. It is also good to define new and simple test methods that can be used regularly by maintenance personnel. Implementing such grounding measurements could be important in an EOS protection program.

Bad grounding can also pose a possible EOS risk to devices during soldering. In a PCB manufacturing line, the tip of a soldering iron was found to be fluctuating and unstable. The values recorded were as high as 100 V in some cases. Again the company was not aware of such a problem and the possible consequences. Therefore, grounding checks (e.g. according to ESDA standard, ANSI/ESD S6.1) should be implemented as an in-house routine check.

Some other examples of challenges in a manufacturing environment are discussed below.

Technology Change

Technology changes in themselves do not cause EOS damage but the techniques used in the manufacturing environment must be considered when the technology changes. An old example, which resulted in EOS damage, involved the use of a simple tool. The technology change was from bipolar technology to CMOS. The tool was a very simple device that was used to troubleshoot opens and shorts. The tool was a simple battery powered circuit tester that lit up when there was a connection and remained dark when no connection was detected. This device was used on PCBs after a failure at a system test level.

If a system diagnostics test indicated a failure, the initial failure analysis would use this simple circuit test tool to determine if there was a short or an open. This was a very simple and quick test done by the system test floor to try to isolate the failure. When the technology was bipolar, this technique worked quite well. When CMOS was introduced the tool was used as before. However, it was found that the current in the tool would cause a catastrophic failure in the CMOS technology. Through failure analysis, the circuits that were traced with the tool were found to exhibit EOS damage. Once the tool was removed, that type of EOS damage was eliminated.

Based on this information, whenever there is a technology change, the tools used on the manufacturing floor should be reevaluated to ensure no damage to the devices takes place.

Tester connections

Testing of subassemblies, such as PCBs before they are assembled into a system, allows detection of defective devices early in the manufacturing process. There are two general tests that are performed at the subassembly level. One is an in-circuit test (ICT) and the other is a functional test where the subassembly is connected to a tester that simulates the signals that would come into the subassembly in operation.

The testers typically have different connections. Usually, the ICT testers use a bed of nails connection where specific connections are made to the subassembly for open and shorts testing between defined circuits. The functional testers are usually connected to the subassembly using the same connection that the subassembly would use in a system. The ICT tester will only test between the points defined. The functional tester would power the subassembly and then exercise the function by sending simulated signals and monitoring the response.

There was a yield issue that required investigation. The subassemblies passed the ICT test and failed at the functional tester. Failure analysis indicated that the subassemblies exhibited EIPD (see Section 3.3). To determine where the damage occurred, the failing subassemblies were then routed back through the ICT and functional tests. The subassemblies failed ICT test the second time they were tested. Since they passed the first time, the failures had to happen after the end of the first ICT test and before the functional test.

The first analysis used functional subassemblies known to be defect free and tested them at ICT and function test. This was done under supervision of the operators and all known good subassemblies passed both tests multiple times. This procedure eliminated the actual test program as the root cause of the problem. Detailed process assessments were done for any external causes which could have explained the damage, such as ESD events. None could be found and the process had ESD controls

in place. While the operators were under supervision, no additional failures occurred and the manufacturing process was allowed to continue.

A few days later, failures were again seen in the manufacturing process. This time the process was observed without the knowledge of the operators. ICT did not seem to have any process deviations. At functional test, it was found that occasionally the operator connected the subassembly upside down. The tester was powered on and the subassembly failed. The operators always noticed that the connector was upside down, powered down the tester and reconnected the subassembly in the correct way. In every case, the subassembly that was connected upside down would result in a failure when reconnected.

The resulting failure analysis showed the same damage as before. The connector outputs were identified on the failing circuit; it was found that when connected upside down, a power line was connected to a signal line resulting in EOS damage.

The corrective action for this particular failure was to ensure all connectors were keyed so that a connector could not be inserted upside down. This fix was incorporated into the system connectors to ensure a proper connection.

Electrical Noise

On a large server, the input/output connections used fiber optic cables and laser diodes for high speed communications. A failure mode started occurring between 45 and 90 days after the servers were installed. The failure mode was a loss of light. Upon return, it was found the laser diode had failed. The initial failure analysis did not indicate an electrical overstress.

Several stress simulations were tried. One simulation indicated that an ESD discharge to the device would cause part of the laser diode to be dark, however, enough light was still being emitted to pass internal testing, system testing and work in the field. The discharge was rather high, the specification for the transmitter was greater than 1000 V HBM. There was no specification for CDM at the time. The failure was a reliability fail similar to the field return fails.

An investigation was started to determine where the discharge could be coming from. After investigating system manufacturing, a review of the supplier manufacturing process was done. In this case, the manufacturing line and process had controls that should have been able to handle this device.

The supplier had done some investigation and as part of the investigation verified that the burn in tester powered up and down in the correct sequence. The signal lines were also scoped to ensure that they were within the limits. The absolute maximum rating for the signal line was given at 5.1 V DC. However, when the scope traces were being reviewed there were some anomalies on the trace that could not be explained. It was decided to review the input signal lines again.

With further investigation it was found that there was AC noise on the DC signals that was not detected in the initial investigation. The frequency of the AC noise was 50 Hz, indicating that it was coming from the AC power grid. Some of the spikes exceeded 11 V. As the duration of the pulses were very short, only a few of the devices would be damaged by these spikes, however, the devices

that were damaged did have a dark spot. This was the same situation simulated in the ESD discharge.

The fix for this problem was quite easy. A simple filter capacitor between the signal and ground eliminated the AC component of the signal line. Once that was installed, the damage was eliminated. The damage was classified as an electrical overstress but only after the investigation was concluded.

7.1.3 Lessons from Product Testing

A supplier of control units for air conditioning systems in cars was facing failures in production, at 0 km (when the unit was tested the first time in the car) and in the field. The root cause was identified to be a non-dissipative carrier used in the testing process. During assembly and test, the board was pressed into a metal work piece carrier to act as a mechanical fixture. The heat sink of a very ESD robust power MOSFET on the board had a resistive electrical contact to the metal carrier which connected the ten boards in the carrier to each other. For a special heat transfer test, the carrier with the ten boards had to be lifted, which isolated the carrier from ground. Through this process, the carrier got charged up to 300 V. The first contact with the tester occurred at the gate of the MOSFET, discharging not only to the contacted device but also the board and all other boards connected through the metal carrier. Depending on the charging level and the test coverage, the damage was found immediately in the production site or in later steps of the control unit's life time.

A corrective action for this charging problem was found after a risk analysis of the assembly and testing process by grounding the carrier during testing through a 10 megohm resistor. This resistance was insulative enough for the test process and dissipative enough to get rid of the charges before contact to avoid a hard discharge.

Without a discussion between the test engineer and the ESD team about what "testing in an isolated way" means, the problem could not have been solved.

7.1.4 Lessons from Field Events

A manufacturer of wireless phones was facing a problem involving the end customer using their phone at home. While picking up the handset from the charging station, the charged user discharged to the housing of the docking station and creating a transient latch-up event inside one of the devices. Since the end user had no chance to detect this, a high current flowed through the device for an extended time, resulting in melting of the circuit. Inside the device, the ESD protection used on the affected pin (an SCR) did its job and triggered to take over the ESD current. Unfortunately, the board designer connected this pin (a voltage regulator) with an on-board supply without any additional resistance. In the case of an ESD strike, the SCR triggered but could not turn off, since the current delivered by the on-board supply was higher than the holding current of the SCR. The current could easily be reduced to below the SCR holding current value by adding a current limiting resistor in front of the affected pin.

This issue could have been avoided if the supplier and the customer (board designer) had communicated on this issue earlier in the design process.

7.2 Automotive Studies

The automotive industry needs 100 % reliable automotive electronics in order to protect human life inside and outside of the car. It is becoming even more important as cars look to drive more and more autonomously. Today, in an average car with a combustion engine, there are about 8000 semiconductors, more than 100 integrated circuits and additionally at least 25 microcontrollers, totaling billions of transistors in a single car, not to mention hundreds of meters of cabling interconnecting many electronics systems susceptible to hot plugging or cable discharge. Zero defects in these electronic devices during automotive assembly, operation, maintenance, and repair are essential. However, in spite of solid automotive manufacturing processes and the robustness of electronics, in some cases electronic components are destroyed. There can be an electrical stress in the application which exceeds the device´s specification (AMR) and also the device´s individual destruction limit.

It is important to note:
If the *application* exceeded the device's AMR specification and the device is damaged, the device is not considered weak prior to being introduced into the application.

All mistreatment and EOS damage of semiconductor devices in the automotive area occur at ground contacts, supply voltage contacts, controller area network (CAN) low, CAN high, LIN bus, or sensor supply contacts of the semiconductor device. All of these are directly connected to the wiring harness of the car. There is no EOS damage risk of the semiconductor contacts inside the electronic control unit (ECU). The energy to destroy the devices comes from the off-board power system or board power supply. Those cases of mistreatment occur every day, all over the world, in many different automotive applications at many different customers´ sites and garages: EOS is a very common issue in the automotive industry, as shown in Figure 85.

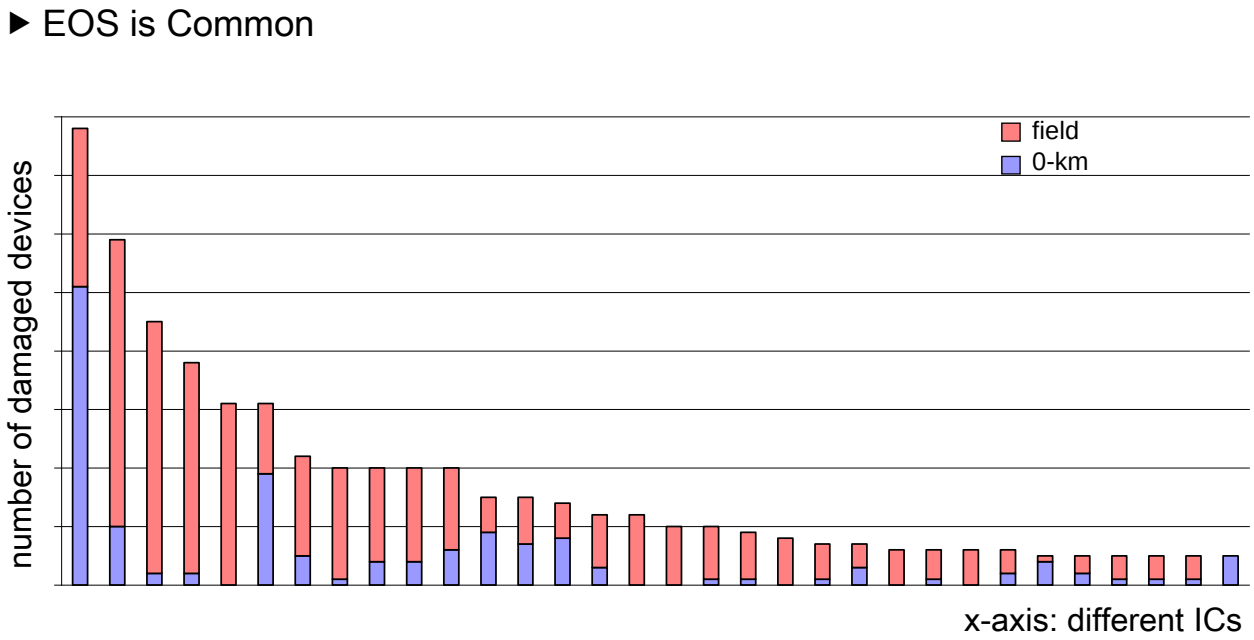


Figure 85: EOS is a Common Issue in the Industry Today

7.2.1 The Primary Reason for EOS in Automotive Industry: Insufficient Awareness

Up until now, there has been no common understanding of EOS in the automotive industry. The customer never intentionally damages a semiconductor. Seldom are there events where enough energy is released to exceed a semiconductor's specification and damage it. If we assume the processes in the automotive industry are safe ~99.999 % of the time, then the path to perfection is 0.001 % or 10 ppm. All of our EOS events are within that 10 ppm. (99.999 % of the time there is no problem and no complaint). This may mean a single person, asked for their own experience, will indicate there is no real EOS problem and is thus not able to judge the reasons and root causes of EOS. The suppliers must be responsible for providing constructive and helpful information and an explanation of events in order to build up enough EOS awareness. Only the supplier is able to collect a large number of individual experiences, summarize and compare all cases.

7.2.2 How can we avoid these Cases in the Automotive Industry?

We need more helpful **communication**. In the automotive industry there are several levels of process partners and interfaces in between as will be discussed in the below sections.

7.2.2.1 Vehicle Manufacturer

The vehicle manufacturer is the final customer (except of course the final owner and driver of the car) of all products. The vehicle manufacturer needs and expects the highest built-in reliability and safety. All suppliers need to fully appreciate this and must understand the applications and environments, even if the vehicle manufacturer is not aware of the critical stress events, and consequently do not describe in detail in the specifications. All involved parties are encouraged to work together with the vehicle manufacturer regarding the application and environment. Not all associates of vehicle manufacturers are aware of EOS and especially of the "remote effects" via ground, battery supply, buses, etc. of stress energy in the system of a car.

7.2.2.2 Engine Manufacturer

This level can produce many critical situations for EOS damage. An engine, which has significant inductance and utilizes wiring harnesses which could possibly already be damaged, is tested with power supplies in cold and hot tests with real ECUs. If, for instance, the hot test is stopped by interrupting the connection to the hot running engine by hot plugging, huge EOS peaks may be created which can easily destroy engine electronics

7.2.2.3 System Manufacturer

Consider, for example, the case of diesel injection, which includes the following in the "system": ECU, common rail, all pipes to the cylinders, the high pressure pump, and the glow control unit, etc. All of these parts are assembled onto or near the engine. This "system" can influence the car electronics around the engine and can also be influenced by stress impact from the wiring harness within the rest of car. All that the system manufacturer understands about the operating conditions, they receive from the engine manufacturer, who in turn receives all their information from the vehicle manufacturer. If the communication is inadequate, the system manufacturer can easily make a design error.

7.2.2.4 ECU Manufacturer

The ECU manufacturer should know about the system for which the ECU was developed. Because there are several interfaces between the ECU level and final customer, this is very challenging. In order to make improvements the ECU manufacturer must investigate nearly all EOS cases to better

understand reality in the 0 km and field environments. On the other hand, it helps to understand the customers´ processes and how avoiding mishandling and mistreatment may reduce EOS risk. While it is not possible to protect a semiconductor against every form of mistreatment, it is important to know the critical process steps in a customer´s subsequent processing in order to avoid any mistreatment. During negotiations it is also important to speak about the definition of EOS.

This white paper lists the most important details about EOS. Now customers, regardless of their level of understanding, can easily read about EOS and its consequences and how to avoid it.

7.2.3 An Example Application in the Automotive Industry

Using Figure 21 from Chapter 3, let's consider how this might apply in the automotive industry using a specific EOS example with four regions of electrical stress and use ESD as an example of how to interpret these four regions as shown below in Figure 86:

- **Region A**
  - Electrical stress between zero and the maximum operating condition
    - The IC is running in a normal mode of operation.
    - No EOS, any failing ICs are considered weak devices.
    - ESD is specified and is a normal "operation mode".
- **Region B (note: in Figure 86 below, regions A/B are combined as a result of an agreed operating range between the supplier and customer)**
  - Electrical stress between the maximum operating condition and AMR
    - The IC is running in a situation in which accelerated aging will reduce the lifetime below the normal quoted lifetime unless appropriate restrictions are followed.
    - No EOS; any failing ICs are considered weak devices if restrictions are followed.
    - ESD is specified and is a normal "operation mode".
- **Region C**
  - An ESD event exceeded AMR but below a destruction threshold for the device
    - Traditionally, this was not accepted as EOS, because "there is no visible damage".
    - It ***is*** EOS, because this event exceeded the product specification.
    - New understanding of EOS: user exceeded the device specification, this is ***not part of the user-supplier contract.***
    - Region C, while not causing apparent damage, exceeded AMR and likely created hidden damage which can lead to future system failure.
    - In this case, the ESD is out of specification, and the result is ***EOS by ESD.***
- **Region D**
  - An ESD event which resulted in exceeding the destruction threshold
    - AMR was exceeded; this is EOS as the device specification has been exceeded.
    - This is the traditional understanding of EOS, because of the visible damage.
    - The device is immediately destroyed.
    - As with region C, this is a forbidden region.
    - The ESD is out of specification and the device is destroyed. In this case of an ESD event, it is an ***EOS damage by ESD.***

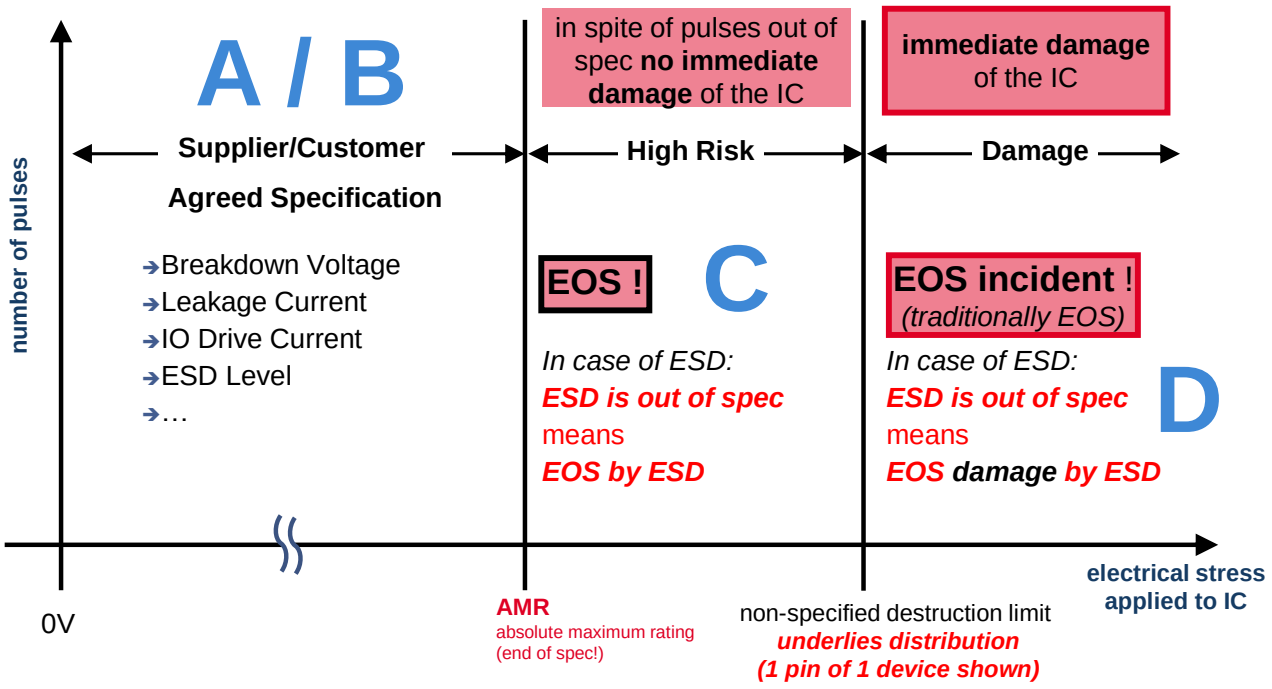


Figure 86: EOS Example Using ESD Leveraging the General Figure 21 of Chapter 3, Note: Sharp Transition between Region C and D due to Depiction of 1 pin of 1 device (no distribution)

Electrical overstress is a result when a maximum limit (AMR) for either the voltage across, the current through, or power dissipated in the device is exceeded and as a result causes the device to be damaged or malfunction (regions C and D, see Chapter 3). In region C, the semiconductor device may have an unpredictable lifetime reduction. Future operation of the device is a *very high risk* due to possible latent damage.

If the stress event was increased, region D will be reached and the device would experience permanent damage as the destruction threshold of the device is exceeded. In this understanding of EOS and AMR, region C is merely a stepping stone to final damage of the device.

Operation according to the specifications is normally guaranteed by the component supplier up to the maximum operating condition. Operation between the maximum operating condition and the AMR (Region B) will not damage the semiconductor device, but reliability may be impacted and full functionality is not guaranteed (unless there is agreement between supplier and manufacturer). If no maximum operating condition is specified, then the AMR equals the maximum operating condition. If no AMR is specified, then the maximum operating condition equals AMR. If there is neither a maximum operating condition nor AMR, no operation is allowed and the customer needs to clear this gap with the supplier, who alone is responsible for defining the device's quality and reliability.

7.2.4 Advantages of this WP EOS Definition for Automotive Applications

The old traditional understanding of EOS expects a visibly damaged device from operation beyond the destruction limit. This understanding is completely covered by region D of our EOS definition.

Only these obviously damaged devices will normally reach the FA labs. If the customer occasionally operates the semiconductor device in region C, there may be no need to complain, because according to the definition of region C, there is no immediate damage.

- In this new understanding, the electrical overstress is extended from region D down to region C. This definition clearly **shows** the **responsibility**. The damage is caused by operating out of specification in the customer´s environment. If the customer operates outside of specification (intentionally or unintentionally), then the customer *must* work with the supplier in order to clarify the root cause.

- The customer needs to **understand** and be **educated**, it doesn't work to decide by a "proven in use" approach. This can sometimes be the case in a consumer electronics environment, but for reliability reasons, it is not possible in an automotive area. The customer is encouraged to discuss and investigate their application conditions with the supplier.

- If, while analyzing a customer´s application, a device is found to be operating beyond AMR but not experiencing physical damage (stress region C), it has clearly still experienced an EOS event and repair should be started while working with the customer to avoid this in the future. A decision about AMR limits is only allowed by the supplier according to their process release procedures. The supplier alone is responsible for the reliability of their devices. The user (customer) needs the supplier´s confirmation of risk and therefore must **inform the supplier about stress levels**.

The biggest advantage of our EOS definition is its **reference to AMR** instead of a destruction threshold. This independence of the destruction threshold allows comparison of two different semiconductor device types with different destruction thresholds, and allows fulfilling the same specification in the same application (region A and region B). If there are operations in region C (which is very common in the field!) one semiconductor device type with a lower destruction threshold would be damaged more often as compared to the second device. In the old traditional understanding of EOS (only region D) a count of destroyed devices might imply the first semiconductor device type is weaker. However, this is not really helpful in root cause analyses, because root cause lies in the application and not in the seminconductor itself, and a root cause analysis may find both semiconductor devices are at risk due to exceedance of AMR.

Consequently, the automotive world does not speak of "EOS failures", but "EOS damage". A device which is operated out of specification cannot "fail", it is damaged or destroyed. Failing is only possible for weak devices operated in regions A & B.

In Summary

The semiconductor device is designed for operation within the maximum operating conditions (region A), and with certain limitations and agreements with the supplier, may be operated across all of region A and B, but was not intended for operation in region C or D!

Key items:

- *Speak to each other, build up awareness, investigate the cases, there is no other way.*
- *Learn about the customers´ applications and strive for congruence between stress and resilience.*

7.3 Integrated Circuit Trends and EOS Effects

7.3.1 Impact of Semiconductor Technology Parameters on EOS Damage

It is often assumed that scaling of advanced semiconductor technologies would have a detrimental effect on the rate of failures which exhibit EOS damage. In this section, we will examine if there is any expected impact from key transistor technology parameters such as silicided diffusions, thinner interconnects, and reduced breakdown voltages for gate oxides and transistor junctions. It is also worth considering whether reduced latch-up tolerance would have an impact on EOS susceptibility.

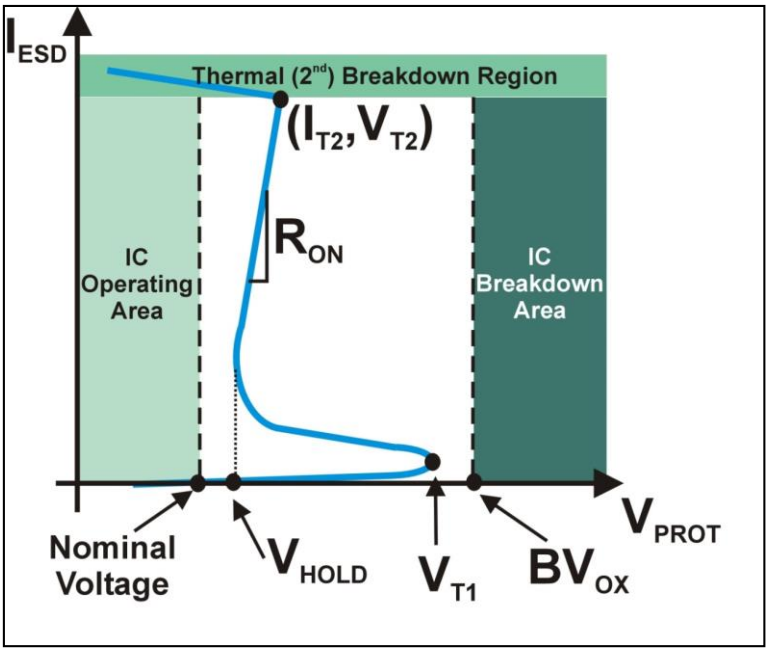


Figure 87: The ESD Design Window

In Figure 87, the design window for ESD protection as well as the relevant transistor ESD characterization parameters are depicted. The desired ESD design current level is on the vertical

axis and the voltage of the protection device is the horizontal axis. The operating voltage for advanced CMOS technologies generally ranges from 1.0 V to 3.3 V. This is represented by the left box known as the 'IC Operating Area." The right hand box, "IC Breakdown Area", represents voltage tolerance of the IO buffer devices with respect to transistor gates (shown as BV_{ox}) or junction breakdown (not shown) voltages. As CMOS technologies have advanced, BV_{ox} has become lower than junction breakdown and has become the critical limit. At the upper end, the thermal breakdown region (denoted by I_{t2} and V_{t2}) is shown. This thermally defined limit may be due to the protection transistor's breakdown under ESD conditions, or it can be defined by a current density limit of the ESD path metal interconnect. A protection device that triggers at V_{t1} (shown in Figure 87) must ideally be below the BV_{ox} limit, and the device must carry enough current to meet the ESD goal before being limited by the I_{t2} at the upper limit. However, if the on-resistance of the protection device is large enough, the V_{t2} point (representing failure) can be reached earlier. If the maximum current density of the metal for the protection device is lower, due to thinning from advanced technologies, it can also hit the failure limit before reaching I_{t2}. In either case, they all form the upper limits. This means that the window between these limits is the available ESD design window.

The protection device should not turn on within the operating region, must trigger before the oxide breakdown, and carry enough current to reach the ESD failure current limit before exceeding the voltage level of BVox. The blue curve in Figure 87 represents one typical protection strategy where the clamp turns on at V_{t1}, holds at V_{hold}, has an on-resistance R_{on}, and has its breakdown at (I_{t2}, V_{t2}) a point which exceeds the ESD target current.

In advanced technologies, this available design window is drastically shrinking in area due to lower BVox, and degraded I_{t2}, as well as lower metal current density under ESD conditions. The implication is that component ESD target levels will have to be reduced for these technologies towards acceptable target levels while still offering safe protection margin in production areas with the proper ESD protection controls. Reductions in BV_{ox} are a result of thinner oxides at the gates that are necessary to achieve higher performance circuit designs. The degraded I_{t2} is a result of shallower junction transistors and the use of advanced materials such as silicides which reduce junction sheet resistance which in turn help high speed designs. At first it would appear that the lower junction sheet resistance would improve the I_{t2} level. This is not true. Low sheet resistances reduce the ability to create ballast resistors to spread current out more uniformly and the low resistance in the silicide tends to force current to flow through junction edges rather than over more of the area of the junction. These effects are summarized in Table 8 below.

Table 8: Technology Feature Size and Process Parameter Impact on ESD Robustness

Feature Size	IC Process Feature	Impact on ESD Robustness
< 1 um	Silicide	Poor thermal resistance
< 250 nm	Leff	Local channel heating
65-90 nm	Tox < 40 A	Oxide stress
22-32 nm	FinFET SOI	Metal current density Channel/FinFET self-heating
10-22 nm	FinFET	Metal current density Interconnect resistivity FinFET self-heating

What does all of this have to do with EOS? If ESD design levels were reduced, would they have an impact on failures which exhibit EOS damage? Intuition would be that EOS could become far worse. Actually, the analysis of field return data (representing billions of IC devices) by the Industry Council revealed that between 500 V HBM to 2 kV HBM or between 250 V CDM to 1 kV CDM the return rates for EOS are uncorrelated [3, 4]. These results included advanced technology products and showed little effect of the technology node or the technology features, such as salicides and thinner oxides, when combined with the data from more robust technologies with higher breakdown voltages. Also noteworthy, the mixture of devices contained more than 600 different designs with VDD voltages ranging from 1.0 V upwards. Technologies ranged from 350 nm to 45 nm and in a wide variety: analog, digital, automotive, dynamic random access memory (DRAM), microprocessor control units (MCUs), power devices, and radio frequency (RF) devices. This in itself is evidence that previous technology scaling does not correlate with an increase in the number of failures exhibiting EOS damage. Implied is that, to a first order, different designs, such as DRAMs or microprocessors, have no correlation to the rate of occurrence of failures with EOS damage. However, as pointed out, design windows are shrinking, and as such, AMR levels are also being reduced. Another possibility for this lack of relationship is adherence to AMR levels.
Other impacts can be considered. For example, do higher levels of component ESD (such as 4 kV or 6 kV) help reduce EOS damage in a system? Second, do the protection clamp styles for component ESD designs have any influence on failure rates for EOS damage? These and other factors will be examined in the next section.

7.3.2 Impact from On-Chip Protection Design on EOS

Although the design of ESD protection is not meant to protect against EOS events, the IC *design style* of ESD protection can indeed influence the rate of failures returned resulting from EOS damage, depending on the particular application and operating environment. This has been observed in the case of wrong protection device types on power supply pins or premature triggering of the ESD devices during use applications. ESD design engineers are not typically consulted by OEMs concerning the risks involved during use applications. They can only protect against those events they are aware of from the application requirements. Even then, the ESD designer is focused only on the ESD cell and protection path through the component. Some design styles involving the

trigger and holding voltages can have more of a system-wide impact as discussed in the next section.

In general, tuning process technology to mitigate unexpected EOS damage from ESD designs is not an option, because the technology is optimized for the IC applications, speed performance and product specification needs. The ESD design comes during technology characterization and matures after the technology has been well established. Thus, any EOS issues arising from specific ESD protection design methods are addressed by either the ESD designer or the IO designer, sometimes both.

7.3.3 Impact from IO and Chip Design Styles

IO design styles vary in their requirements for buffer speeds and drive strengths. In some cases these can lead to designs involving very large output transistors. It is yet unknown whether very large transistor drivers are more likely to have increased risk of EOS damage due to their lower on-resistance. On the other hand, mixed voltage designs involving system-on-chips (SoCs) typically have multiple power supply voltage levels. Thus, power sequencing often becomes an issue. Even with careful power sequencing specifications issued, are there any hidden or parasitic on-chip scenarios that can lead to forward biased junctions? The more complex the design of a chip (especially SoC with multiple power domains), the more likely that unintended parasitic paths can exist. Unless careful design techniques are followed, returns exhibiting EOS damage could be seen. The ESD protection design must take this into account.

7.3.3.1 Snapback Devices

Consider first the so called snapback devices that are used for effective protection at the IO pin or on power supply pins. A typical device I-V curve taken with a 100 ns TLP is shown in Figure 88. The protection device triggers at a voltage of V_{t1} and a corresponding current level of I_{t1}. At this point, the device goes into bipolar snapback mode to hold at V_{hold}. Then, due to the on-resistance with the bipolar in conduction, the voltage rises to V_{t2} and the current to I_{t2}. At this point, the power dissipation causes the transistor junction to fail, or, if V_{t2} is above the oxide breakdown, damage to the input gate can occur. The critical aspect of the protection design is to make sure that the maximum VDD is below that of and not close to V_{hold}. Otherwise, the ESD protection device (if accidentally triggered due to an overvoltage) can draw current and create a fail resulting in EOS damage. As illustrated in Figure 88, design 1 is relatively safe, whereas design 2 is risky due to the proximity of V_{hold} to VDD max. As a general rule, the V_{hold} should be 1.2 to 1.5 times higher than VDD max. This discussion assumes that the VDD does not have severe spikes such as from a noisy power supply. In such cases, the Vt1 will also have an impact.

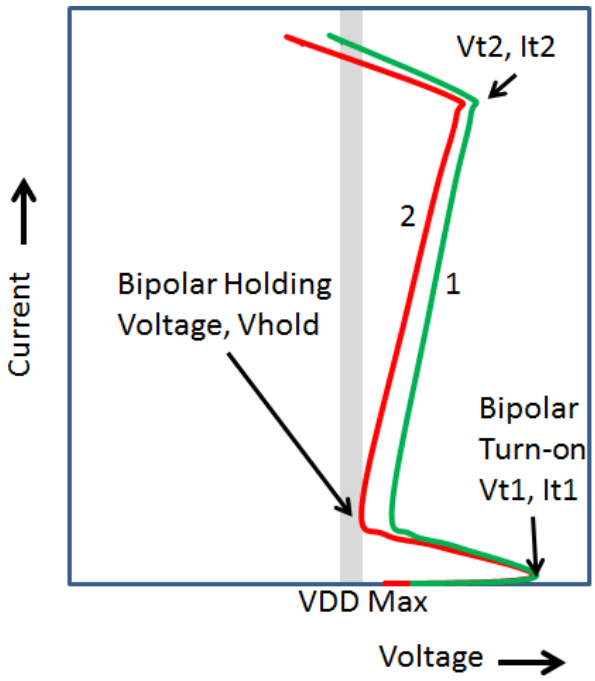


Figure 88: Characteristics of a Snapback ESD Protection Device

A second strategy is to suppress the accidental triggering mechanism of the protection device as much as possible. There are several ways to control this:

i) watch out for rate-firing events of the circuits (known as dv/dt triggering or rise time sensitive circuits)
ii) design techniques with substrate bias (to reduce the possibility of substrate voltage buildup leading to forward bias junctions)
iii) remove nearby sources of current injection like a forward diode to VDD; or
iv) strategically place guard rings to have predictive triggering.

These design suggestions can have some negative impact on the maximum ESD protection level, but often there is enough margin for safe ESD design levels such that avoidable failures exhibiting EOS damage can be minimized at the expense of somewhat reduced ESD performance.

7.3.3.2 SCR Devices

These devices (operating as latch-up (regenerative PNPN) devices with their low holding voltage) are often more effective than snapback devices for ESD protection (see Figure 89). When SCRs are used for IO pin ESD protection, usually precautions are taken so that the junctions are not forward biased in order to avoid SCR action during IO use applications.

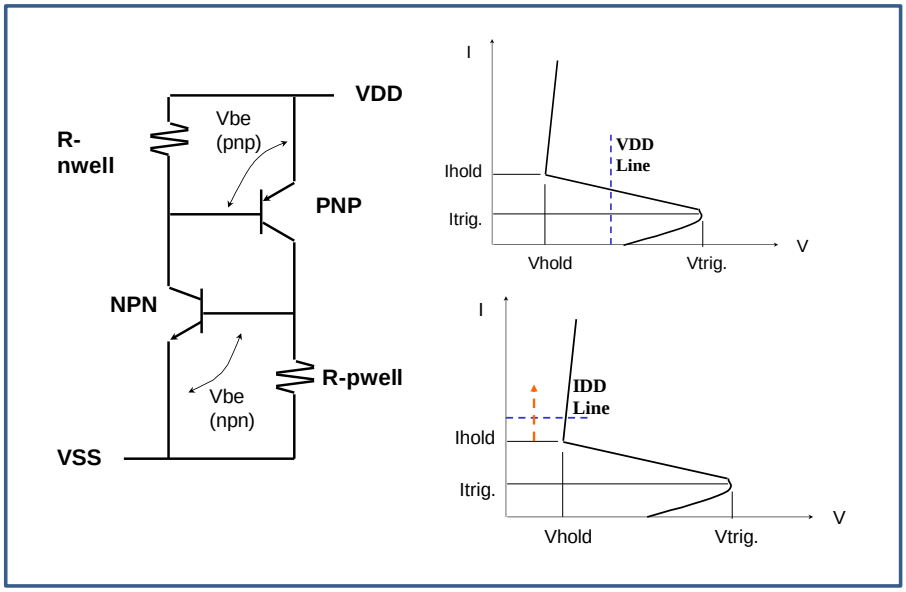


Figure 89: SCR Protection Device and ESD Characteristics

However, SCR devices are dangerous if used for VDD power protection. During IO operation, a considerable amount of substrate current injection takes place. SCR VDD devices, if near IOs and even with trigger voltages sufficiently above the VDD voltage, can accidentally trigger and cause EOS damage. They are safe only on the VDD pin if designed to have the V_{hold} above the VDD_{max} or the I_{hold} above the current level available from the voltage source. Even then, SCRs should be avoided for power protection. SCRs are sometimes used on Ethernet VDD pins but care has to be taken that the V_{hold} is above VDD_{max}. Otherwise, during a cable discharge event, the parasitic SCR can trigger, causing EOS damage.

Another example of EOS damage with SCRs involves their connection to tied-off or unused IO pins. As already mentioned, using SCR protection devices is fine for IO pins but not for VDD power pins. Suppose during use applications a customer decides to tie-off unused IO pins to VDD. Then an SCR device ends up being connected to the VDD domain. This has been known to cause EOS damage. In these cases, it is important to work with the application engineer and recommend tying the VDD connection through a current limiting resistor so that the maximum available current is less than the minimum holding current (See Figure 89).

However, if trigger voltages are above AMR, and there is adherence to keeping V_{hold} above the maximum operating voltages, *SCRs can be a very safe ESD protection device*.

7.3.3.3 Substrate-Triggered Devices

As mentioned above, substrate-triggered devices can pose a potential problem for EOS if not designed correctly. Two such devices are shown below in Figure 90. Both are effective for ESD protection, but their impact on EOS has to be considered. In Type 1, the diode to VDD is placed close to the grounded gate NMOS to effectively trigger the substrate during an ESD event. But it has been observed that during burn-in, noise spike injection into the VDD at higher temperatures can create unexpected EOS damage. The Type 2 device shown is a safer design since no diode to VDD is involved. But bringing the diode too close to the NMOS can still cause it to latch.

Therefore, if any customer failures exhibiting EOS damage are involved, these designs must be scrutinized.

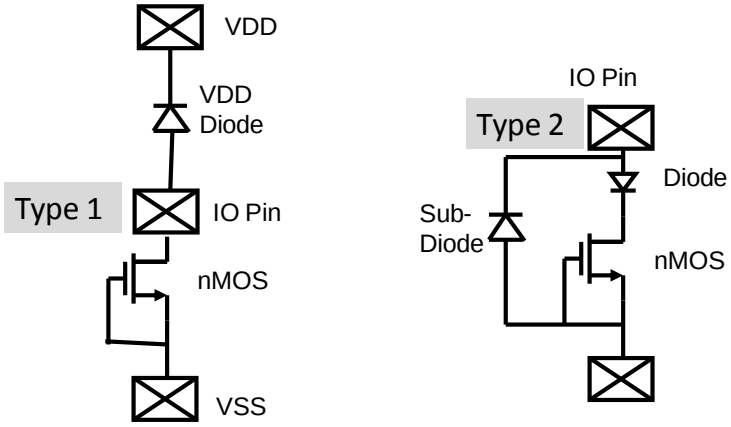


Figure 90: Design of Substrate Triggered Protection Devices

7.3.3.4 Mixed Voltage and Voltage-Tolerant Protection Designs

In some cases, when the power supply pin is at a lower voltage than the maximum IO pin application voltage, higher voltage tolerant designs are necessary. In this case, a stack of diodes may be placed in series from IO to VDD as shown in Figure 91. However, if the wells of the diodes are floating, they can effectively form a parasitic SCR with the pull-down NMOS devices and cause unexpected EOS induced damage [5]. One option to prevent SCR turn-on is to place an N-well guardring for the first diode tied to the pad and to place the other series diodes in the path inside an N-well guardring that is tied to node A. This illustrates an effective design technique to lessen the chance of parasitic-induced EOS damage in mixed voltage technologies.

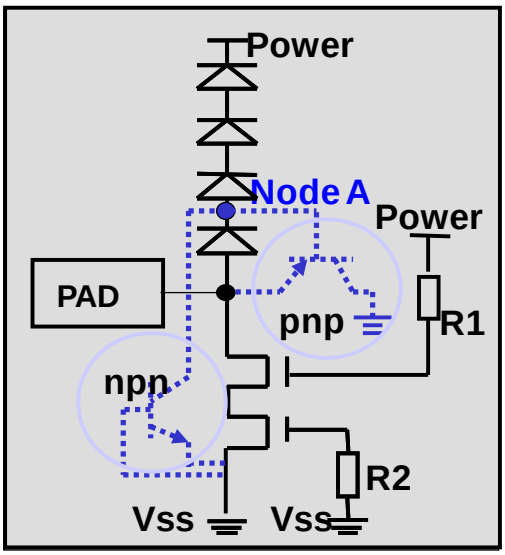


Figure 91: Design of High Voltage Tolerant Protection showing Potential Parasitic SCR Formation

7.3.3.5 Non-Snapback Designs

A presently popular design trend for large groups of digital IO rings rail clamp VDD protection devices where the MOS devices operate in the normal linear and saturation regions and no bipolar snapback of the device is involved. Even in these cases, EOS damage can be an issue if the design does not properly address certain scenarios. The schematic shown in Figure 92 involves an active MOSFET as the rail clamp device between VDD and VSS. However, during normal applications the slew rates from IO transitions seen on the power supply can potentially trigger this device into a latching mode. See Chapter 5 Section 5.11 for an illustrative example.

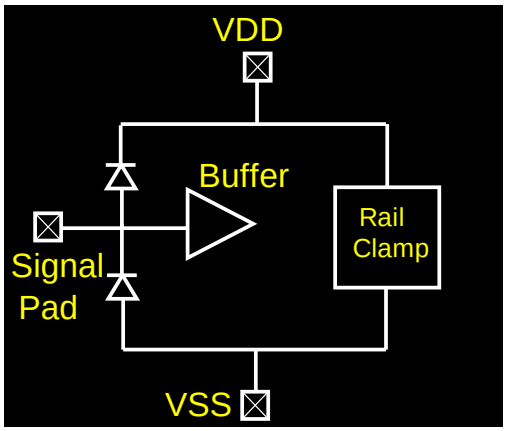


Figure 92: Design of Rail Clamp ESD

7.3.3.6 Parasitic Devices

There could be formation of unintended parasitic SCR devices or forward biased diodes during an IC design. During the actual chip design, there could be instances where the IO cell can have parasitic latching devices. By defining proper spacing rules, placement, and connectivity of guard rings in the design layout, the IO designer and ESD designer can work together to avoid such scenarios. Another scenario is the unintended formation of internal forward biased diodes during power sequencing. As shown in Figure 93, the well connection of the PMOS buffer device to VDD1 could be blocked by connection of its N-well to a different supply (VDD2) than from its source connection (VDD1). The same design situation can occur internal to the chip; depending on the specified power sequencing, the parasitic diode between VDD1 and VDD2 could get forward biased and lead to EOS damage. Thus, proper communication of the design methods used and the risks involved during product use applications is important.

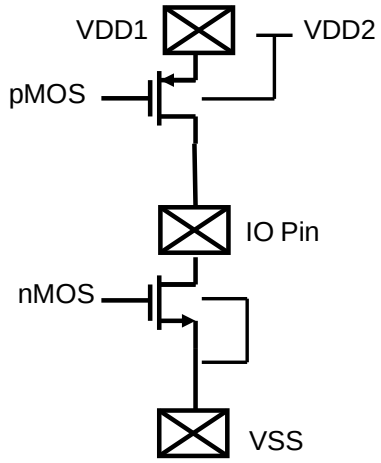


Figure 93: IO Buffer with a Blocked Well Connection

7.3.3.7 High Voltage Designs

ESD devices protecting high voltage designs have increased power dissipation in the turn on mode as compared to those in low voltage designs. As such, when the device fails to protect or when the ESD device itself fails, considerably more energy is available to cause material damage in the failed region. Some correlation has been noted between EOS damage and the operating voltage or environment the devices are designed into. To provide better isolation and to limit parasitic interaction, devices need to be spaced further apart, have good guard band ringing, correctly spaced and connected deep wells to proper voltages, and also have good connections in the substrate to limit substrate voltage drops. Additionally, metal connections between devices and their supplied power or ground must be wide and not have sharp corners and spacing between metals of opposite polarity with wider than minimum design rules. Also, care must be taken to ensure metal overlap of junctions does not decrease breakdown voltages of those junctions due to field oxide interaction.

7.3.3.8 Designs with Impact on EOS

Design styles can sometimes lead to avoidable EOS damage. Some questions which may follow:

Q1: If you use snapback devices for ESD protection, how much room do you normally leave between the ESD device trigger voltage (V_{t1}) and the application voltage for the pin?

Recommendation: This depends on the technology. Normally, it is better to leave about 20 % margin for all technologies, but this may not be practical for higher voltage technologies of > 50 V.

Q2: Do you observe that designs with snapback devices have higher failure rates showing EOS damage?

Recommendation: In general, this depends on the design style and the conditions. If snapback designs do show consistent patterns, consider switching to a rail-clamp approach but with caution. Rail-clamp devices can be especially susceptible with "latch-type" designs. As always, if the problem is identified, the design can be modified to alleviate these types of design related EOS damage.

Q3: What is "injection induced breakdown voltage (BVii)" and how is it helpful in reducing EOS damage?

Recommendation: BVii is a measure of voltage breakdown for MOS devices in which current is flowing in the channel because the gate is biased, as would be expected for buffer devices and clock devices. If this voltage is too low, accidental latch-up and subsequent EOS damage could happen. This value can be characterized for the process technology by applying 0.5 times VDD on the gate of a typical NMOS transistor and measuring its avalanche breakdown. BVii should be ideally >1.5 times VDDmax to avoid latch-up and eventual EOS damage at high temperature operations.

Q4: Can products designed with 4 kV or 6 kV HBM show relatively more returns for EOS damage than products that meet only 1 kV or 2 kV? Do these failures appear as massive damage in the protection devices?

Recommendation: This is possible depending on the pin types or the handling procedures. It is generally not a good idea to place such high ESD protection on interface pins or on VDD pins. If massive damage on protection clamps is seen then something is wrong. Investigate whether these clamps are overly responsive to any glitches or transients. Consider redesigning to lower ESD level clamps in this case.

Q5: Are SCR protection devices demonstrating more frequent EOS damage?

Recommendation: The use conditions must always be known. If this issue is seen, then confirm whether the holding voltage is too low (that is, less than the VDD voltage). Redesign the SCR protection with a higher holding voltage by placing 1 or 2 diodes in series with the cathode and/or adjusting the P+ guarding spacing. Also note that while SCR devices might be okay on IO pins, if they are tied off to VDD as unused pins, there could be accidental EOS damage due to noise spikes on the VDD supply.

Q6: With respect to the above, would you forbid SCRs on VDD pins?

Recommendation: If you must use an SCR device on VDD pins, make sure its holding voltage is clearly higher than the VDD voltage. Otherwise, opt for a different type of protection clamp. RC triggered NMOS clamps are safer as long as they are latch-less and do not trigger under slew rate tests.

Q7: Do you have any specific design rules which should be communicated to customers so as to minimize accidental EOS damage?

Recommendation: Inform customers to use: 1) extended ground pins on connectors, 2) transient voltage suppression (TVS) Zener diodes which are compatible with AMR limits, and 3) circuits that limit residual voltages to the IC pins.

Q8: Are high voltage analog designs more susceptible to EOS damage?

Recommendation: It is possible that some high voltage designs experience a relatively higher rate of failures exhibiting EOS damage. In this case, make sure that the SOA is understood. It is important to understand that many low voltage integrated circuits can withstand voltages 50% or more above their maximum operating voltages but this clearly depends on the window of tolerance and is device specific. Refer to Region B of Figure 21 which sets the region between maximum operating voltage and the AMR. For high voltage technologies (>> 5 V), the tolerance could be reduced to as little as 10% for some devices.

7.3.3.9 Ground Connections

There is also potential risk involved with floating connections, **ground bounce,** which causes forward biased diodes, loss of ground, causing substrate bias and triggering of parasitic NPN or PNP transistors which can lead to SCR turn on. For example, consider a two die single chip IC solution consisting of a digital die with high IO pin count and an analog/digital (A/D) converter which might share the same ground. If the digital IO were to be configured to initially drive all logic signals high and suddenly all IO were configured to drive logic low, this could create a pulse on the common ground which could rise significantly above a 0.7 V potential during the brief time the IO were switching. This could cause the sensitive analog die grounded substrate to forward bias and cause parasitic interactions within the circuitry. For this reason, it is recommended to separate the analog and digital on-die path by at least a forward diode drop in each direction. High current analog circuits are commonly susceptible during high current switching modes and hence require special attention.

7.3.3.10 IO Impedance Effects

It should also be briefly mentioned that during the standard JEDEC latch-up test (described in JESD78), EOS damage could occur at the IO pin if certain conditions are not understood. For example, if the IO pin has a high input impedance, forcing current for a perceived latch-up test can lead to EOS damage. This is shown in Figure 94. In the example shown, if a customer requires deliberately forcing greater than 70 mA (with a 100 mA pass requirement) into the pin to check for latch-up, it could take the protection NMOS or the output NMOS into a breakdown damaged mode resembling EOS damage. Once the voltage reaches the specified maximum stress voltage or 1.5 times the VDDmax (whichever is lower), the test must be stopped.

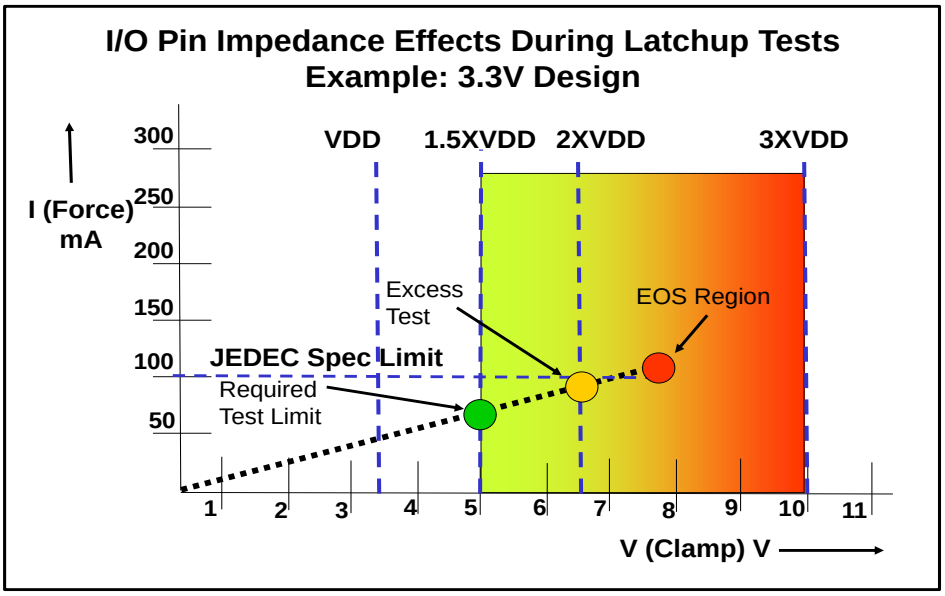


Figure 94: Example of EOS risk in JEDEC Latch-up Testing

7.3.3.11 Summary of IO Design Styles and Impacts

This section has discussed many different design styles, their advantages and disadvantages and things to consider. Table 9 summarizes this discussion.

Table 9: Summary of Design Styles and Their Impacts

ESD Protection Style	Applications	Advantage	Impact on EOS	Cautionary Notes
Snapback Devices 1. GGNMOS 2. GCNMOS 3. Sub Trig. NMOS 4. SCR Devices 5. MOS integrated SCR types	• Fail-safe* IOs • Analog designs • Mixed voltage designs • High voltage designs	Often can achieve high ESD levels 2 kV to 4 kV HBM	Higher probability especially for >4 kV HBM	• Dangerous if device triggers with low margin to application voltages • Prone to latchup effects without careful guardring placements • Must be compatible with AMR specs • SCR not suitable as VDD protection
Rail Clamps 6. RC timed NMOS 7. RC timed PMOS 8. RC timed DENMOS	• Non-failsafe • Low Cap designs	Compatible for high speed designs and provide 1-2 kV HBM	Moderate probability	• Prone to unexpected triggering under VDD slew rate conditions causing either latchup or EOS damage • Must be compatible with AMR specs
On-chip IEC System Protection 9. Large GGNMOS 10. Large SCR	• Special interface pins • Antenna pins	Meet 8 kV IEC test With savings on PCB design	Moderate to high probability	• Dangerous if triggered under EOS since have very low on-resistance • Must be compatible with unknown external diodes if placed • Can have severe ground bounce effects

*Fail-safe means no diode between IO and VDD supply is allowed

7.3.4 Summary of Technology/Design Impact

After an examination of returns with EOS damage, it became evident that technology scaling (from 350 nm to 45 nm) did not show any impact [3, 4]. Although this is somewhat surprising, it could be argued that these technologies operate at lower power supply voltages where the relative variations may not be that significant. But this observation is based on limited data. It should be cautioned that further technology advances with thinner gate dielectrics and novel transistor process technologies will reduce breakdown voltages and continue to shrink design windows. This reduction in breakdown voltage will reduce AMRs and may subsequently begin to influence returns which exhibit EOS damage. In any case, it will become even more critical to continue adherence to the AMR boundaries and maintain clear communication between supplier and customer. The introduction of newer technologies, such as FinFETs, may change this scenario because these transistors are susceptible to thermal effects. But these issues will not be clearly known until future products with these transistors are in volume production. Nevertheless, continued adherence to the AMR boundaries will be critical in all cases.

The impact of ESD protection design has been discussed in this chapter with a few illustrative examples. However, it should be noted that, generally, with advanced technology models the AMRs are being lowered while external application voltages remain the same. As a result, more focus should be shifted to determining if there is a correlation between the type of protection design and the rates of damage due to EOS.

Low Voltage versus High Voltage Technologies

There is another aspect of return rates that should to be considered. Smaller feature technologies exhibiting EOS damage might display a relatively large amount of damage. But this might not necessarily lead to higher failure rates for EOS damage. For one thing, low voltage devices do not suffer frequent failures from operations that are out of specification. In contrast to low voltage technology products (1 to 3.3 V), high voltage technology products (especially, 20 V and above) might see relatively higher rates of returns exhibiting EOS damage. Consider, for example, a low voltage technology which is normally operated inside an ECU, protected against EOS. That means there is only a weak outside influence and so there may be no increase in EOS numbers or cases. On the other hand, high voltage devices are connected via a wiring harness to the rest of the automobile. Here the supply voltage is always the same (12 V or 24 V) and all EOS events from outside the ECU are happening independently from the semiconductor technology. It should also be noted that high voltage technologies must survive larger supply voltage variations and employ different types of protection devices than are commonly used for low voltage technologies.

Summary of Technology Impact

These observations infer that different technologies will be damaged with different probabilities. It is safe to conclude that the actual technological impact is not completely clear. It may depend on other market segment applications which have not yet seen devices with very advanced technologies, or it may surface as more products with very advanced technologies move to volume production. Nevertheless, following some of the guidelines given here can always help to mitigate failures exhibiting EOS damage to some degree.

Design Issues and Margins

As described in this section, the design of IC on-chip protection can potentially play a role in creating avoidable failures exhibiting EOS damage. On top of that, lack of proper communication about the safe range of application voltages can further exacerbate the problem. The important points for improving communication are outlined in Section 7.4.

With these advanced technologies, the impact on EOS damage in regard to design margins may need to be carefully considered since AMRs would simultaneously be reduced. While some of this can be alleviated with better adherence to the relative AMR values, the designers should also take some responsibility to mitigate EOS damage in applications. For example, using better modeling and simulation methods to increase predictability of the clamp behavior under various transient conditions in conjunction with increasing demand for better process technology control so that the breakdown voltage fluctuations are well understood and are anticipated ahead of the design. This breakdown aspect can become equally critical for high voltage technologies where the breakdown voltages come closer to design applications. In all cases, where necessary, the design styles have to be scrutinized to make sure that reduced AMRs are not going to have unwanted effects on EOS damage returns.

While it is important to avoid EOS damage in the design phase, EOS damage events do take place in the field during various applications for various reasons. In some cases, field damage might even be related to the ESD designs as illustrated below. Following these illustrations, in the next few sections some lessons from factory, product testing, and field events will be presented. Finally, automotive application examples offer a wealth of lessons to minimize and avoid EOS damage. In examining these cases, it is important to first understand that the automotive industry has a unique perspective on EOS margins and the resulting EOS damage events. These are dealt with in detail in Section 7.2.

7.4 Communication with Customers

It becomes evident with the list of example cases of EOS damage in various scenarios, from IC protection design to factory and field as well as automotive environment events, that much of it can be avoided by proper upfront communication. Corresponding recommendations are given in this section.

From the discussion on IC design and applications that can lead to avoidable cases of EOS damage in Section 7.3, it can be seen that it is possible to provide a recommended checklist of system per-pin conditions.

Clear communication between the **IC Customer** and **IC/ESD Designer** should contain critical details as shown below in Table 10. This is necessary to avoid problems from IC ESD designs. The following items and schedules are recommended to minimize confusion and misunderstandings.

Table 10: Mitigating IC ESD Design/Application Causes through Clear Communication

IC Customer	IC/ESD Designer
Specifications to be Noted • Max Operating Voltage • Overshoot range • Undershoot range • Tie off on IO pins	Design Approaches • Proper margin to VMax • Knowledge of trigger and holding voltages • Devices in full Safe Operating Areas • Proper selection of ESD cells
Applications to be Noted • Power Sequencing • Pin biased above/below supplies	Precautions • Watch out for internal parasitic diodes • Proper designs to accommodate bias ranges
Aware of Transient Risks • How are they created; what is expected • Hot-plugging	Design Strategies • Designs not to trigger during transients • Making sure dV/dt are not in ESD regimes
Communication • Meet and discuss before design start • Update any new changes	Interaction • Ask all proper questions • Seek information before freezing design

Next, we consider observed EOS damage problems that could come from applications which can be misconstrued as being related to ESD design. Chapter 5 presented several case studies that indicated EOS damage on returned devices which were first perceived as ESD design issues but careful analysis showed many of the problems have been a result of misapplication. This again illustrates that thorough analysis followed by proper communication are important considerations, as shown below in Table 11.

Table 11: Proper Communications to Resolve FA Results

IC Supplier	Applications Engineer
Initial questions to ask • Is there more than just one FA per incident? • Is there conclusive FA beyond optically observed damage?	Information to provide • Confirm if the same type of damage is seen on more than one incident • Work with the IC supplier to make sure the damage details are clear
Clarification • Narrow down the specifics; ask where the problem started • Origination of the problem; ask when the problem started	Interaction/Information • Inform where the problem started (during assembly, testing, production, use,..?) • Inform when the problem started (during product introduction, tool change, flow change, application change,…?)

Understanding the problem
• Can this be replicated through:
  • Power profiles?
  • Qualification tests?
  • Bench set-up?
  • In-situ data?
	1st Phase Alignment
	• Understand how the supplier tried to replicate the problem
	• Understand and discuss the results
	• Agree if a bench set-up is realistic
	• If possible, give access to voltage and current observations in-situ

Consequences • Damaged parts in other applications? • Do they show the same issues? • What differences and commonalities?	Interaction/Information • Give critical information on other products or if the same damage in other applications • Inform about any glaring similarities
Final Resolution Keep asking until a final resolution is achieved	Final Alignment Provide feedback on satisfaction to the final resolution

For many of the factory and field returns diagnosed as having EOS damage, establishing communication procedures can help to avoid future issues. These problems can be especially severe during automotive applications, as presented in Section 7.2. To accomplish this, a general communication format with checklists, as shown in Table 12, should be useful in many market segments, including automotive.

Table 12: General Communication Table for Resolving EOS Issues

Issue	Action/Resolution
Damage after packaging	Are proper grounding procedures followed? (create a checklist)
Damage after assembly & test	Risk analysis of the assembly established?
Damage from a field event with unexpected power connections	Communicated with supplier to confirm safe connections to on-board supply?
Hot-plugging	Is first-mate-last-break always followed?
Unexpected EOS from ESD	Is a balanced ESD strategy followed to avoid charging/discharging events?
Mechanical overstress of cables leading to electrical damage	Are safety procedures available to avoid these scenarios in assembly?
Improper grounding of tools	Are proper guidelines in place and followed?
Outsourcing to contractors	Established training on EOS situations?
Understanding of EOS Environment Semiconductor manufacturers must comprehend all applications for the semiconductor device and all operating conditions	**Aligning / Educating / Training** Customer/Suppliers treat all conditions as a contract Agree unspecified conditions are not allowed Educate all parties involved with training on EOS

7.5 Recommendations for EOS Minimization and Mitigation

One recommendation for system manufacturers is to provide extended pins on both boards and cable connections for ground and supply pins. For example, a safe connection methodology would be to ensure ground pins connect first, followed by supply pins, with the last connection applied to the IO pins. This would ensure that a ground path exists first when connecting, that supply is not connected before ground (which would cause "shoot through" current), and also that both power and ground are connected before IO, ensuring that IO pin connections cannot connect first, causing shoot through to supply or ground. It is also recommended where possible that connections not be made in "live" or "powered" conditions.

7.6 Conclusions

Mitigation of EOS can first be addressed by understanding the impacts of advanced technology scaling and the IC ESD protection design methods. Even if all the design methods are properly done during applications, cases of EOS can appear from factory and field events. The most severe form can come from automotive applications.

This chapter summarized the impact of technology scaling, where to date, the technology advances per se are not the real problem. Rather, EOS scenarios can come from incompatible ESD protection designs or choices of protection structures. Much of this can be mitigated by asking the proper questions before implementing ESD in IC devices. It is important to remember that there are multiple application scenarios where EOS problems can be avoided by understanding the cause of the problem and establishing procedures to be followed.

EOS damage events that take place in the field from various applications and for various reasons were also presented. Understanding of lessons learned here from factory experiences, observations during product testing, and in some cases specifically from recorded field events could mitigate many EOS damage cases.

Finally, the automotive world has a unique perspective on the AMR window. Only through understanding this perspective, and that low tolerance to EOS damage in any automotive application is a serious issue, can one derive better methods for diligent practices as well as define effective means of communications between the various partners that deal with automotive products to mitigate EOS damage during automotive applications.

Based on the divergent examples presented here, along with the detailed case studies from Chapter 5, some clear guidelines for communication have been presented. These involve active communication between the ESD Designer and the IC Customer to ensure that no design related issues lead to unnecessary EOS damage. In regards to product failure returns and their analysis, proper and effective communication between the IC Supplier and the Applications Engineer becomes crucial. For addressing factory and field returns and subsequent resolutions, additional forms of communication are needed to understand and avoid the same EOS problems. Finally, automotive issues can be equally resolved with the same effective communications methods as outlined in this chapter. In every case, all of these should be accompanied with a good training program.

References

[1] Salcedo-Suner, J.; Cline, R.; Duvvury, C.; Cadena-Hernandez, A.; Ting , L.; Schichl, J., "A new I/O signal latchup phenomenon in voltage tolerant ESD protection circuits g. " Reliability Physics Symposium Proceedings, 2003. 41st Annual. 2003 IEEE International, pp. 85 – 91.

[2] KP Yan, R. Gaertner, CY Wong; Poor Grounding – Major Contributor to EOS; EOS/ESD Proceedings 2012

[3] Industry Council on ESD Target Levels, "White Paper 1: A Case for Lowering Component Level HBM/MM ESD Specifications and Requirements," August 2007, at http://www.esda.org/IndustryCouncil.html or JEDEC publication JEP155, "Recommended ESD Target Levels for HBM/MM Qualification", www.jedec.org

[4] Industry Council on ESD Target Levels. "White Paper 2: A Case for Lowering Component Level CDM ESD Specifications and Requirements," Revision 2, April 2010, at http://www.esda.org/IndustryCouncil.html or JEDEC publication JEP157, "Recommended ESD-CDM Target Levels", www.jedec.org

[5] KP Yan, Reinhold Gaertner, "An Alternative Method to Verify The Quality of Equipment Grounding", EOS/ESD 2005.

Chapter 8: Summary and Conclusions

Charvaka Duvvury, Texas Instruments (Retired)
Robert Ashton, ON Semiconductor

This white paper establishes the following important conclusions about an EOS definition and the causes that can often lead to EOS.

1. Although EOS has been dealt with historically by many authors, it has never been fully understood nor has it been accurately and thoroughly explained or interpreted.
2. It should never be assumed that meeting ESD levels beyond the specification targets will somehow reduce the rate of EOS returns. There is overwhelming data from the Industry Council to support this assertion.
3. Industry wide surveys have indicated that:
    a. EOS is the most common attribute of reported returns.
    b. The vast majority of respondents indicate that "damage signature" is used to determine EOS.
    c. EOS almost always represents permanent damage.
4. The surveys also conclude that the most common cause for EOS is misapplication, followed by violations to the absolute maximum rating and exposure to electrical stress events during assembly and in the field which violate the AMR.
5. To date, there has been no universally accepted definition of EOS, but the common language as established in this white paper should foster better communication within the industry in addressing EOS problems. This definition can be stated as: *"An electrical device suffers electrical overstress when a maximum limit for either the voltage across, the current through, or the power dissipated in the device is exceeded and causes immediate damage or malfunction, or latent damage resulting in an unpredictable reduction of its lifetime."*
6. Absolute maximum rating requires a more in-depth definition which informs the customer that exceeding the AMR value has associated risks and can lead to irrecoverable device damage. Also, an EOS event occurs if any AMR is exceeded for any period of time.
7. Any specification for AMR has to include constraints for excursions in system operation and environmental conditions which need to be accomodated by system design to allow safe operation and handling of semiconductor components.
8. The electrical and environmental conditions for which the AMR values are intended have to be documented in the datasheet.
9. In systems with unique requirements, the values of AMR have to be provided by the semiconductor component supplier according to the electrical and environmental conditions given by the system manufacturer.

In developing an understanding of EOS, the most important step importance is to first comprehend the root causes. The three main categories for EOS occurrences are during: 1) unpowered handling,

2) powered handling, and 3) switching / AC application. For unpowered handling, the root cause may be related to ESD-like charging and discharging but not related to any HBM or CDM ESD target levels. For powered handling situations, the events may be related to overstress-induced phenomena in which power is turned on, overvoltage, electromagnetic interference, or power upset. Hot-plugging during testing and assembly is also included in this category. For the category of switching / AC operation events, examples may be EOS from RF coupling or spurious EMI. With these multiple causes, it is recognized that EOS origin is indeed very complex, but understanding each kind requires a consolidated effort.

Case studies from customer returns provide a wealth of information to assess causes of EOS damage and also an opportunity to document lessons learned. We have presented several cases of product returns that have EOS damage signatures and have been traced to their root cause. Such analysis to root cause provides a lot more information about the understanding of an EOS occurrence than failure analysis alone and shows that appropriate solutions can be identified to meet customer satisfaction. A step-wise program is needed with an understanding that failure analysis only provides a damage signature but is unlikely to reveal the true root cause on its own. Also, when testing for damage after ESD testing, any violation of AMR (such as during curve tracing as discussed in Chapter 5) is an EOS event which can result in erroneous ESD qualification failures. For these reasons, EOS damage signatures should be analyzed to see whether they are from misapplication, hot-plugging, ground bounces, supply switching, EMI transient surges, or by process, product, or system assembly issues.

Over the last 30 years, technologies have advanced rapidly with transistor scaling and demand for higher speed circuits. For analog designs, mixed low and high voltage technologies have become much more popular. At the same time, these advances have also led to a reduction in component ESD target levels for HBM and CDM to more practical but safe levels. These advances have raised the speculation that EOS return rates would go up. However, we have shown that this is not the case. But independent of the technology or design application, the design of ESD protection devices can have an influence on the EOS return rates. Some recommendations to avoid unnecessary EOS damage events caused by overdesign for ESD have been identified. The purpose of these recommendations is to ensure a safe product design is released to production while mitigating later EOS events in the field or during applications.

There are now an enormous number of factories and assembly areas across the industry. Thus, greater care and discipline to avoid unexpected EOS events must be followed. Some of these highlights include preventing poor grounding methods, practicing better communication between the supplier and the board designer, and avoiding hot plugging, which can be mitigated by practicing the principle of first-mate-last-break. The concerns about EOS in the automotive environment have to be given special consideration. The use of advanced electronics in automobiles is increasing rapidly and not just in infotainment systems but in critical system functions including those important for safety.

The final focus of this white paper has been to emphasize communication methods and training strategies to avoid EOS as much as possible. These continuous communications must be held first between the IC Customer and the IC ESD Designer to make sure that the design approaches are compatible with customer specifications such as maximum operating voltage, expected overshoots and undershoots, and other application scenarios. Next, there must be a clear understanding of and strategy to deal with unexpected transients, hot-plugging events, etc. When units are returned with

any type of EOS damage, there must also be continuous communication between the supplier and the applications engineer to understand the root cause, attempts to replicate the problem and to reach a final resolution. Many of the factory and field event returns likewise need extensive communication to address the specific underlying root cause so that it is not repeated. To this effort, numerous guidelines have to be established and training programs have to be initiated to keep workers up to date. These latter issues become even more important where outsourcing becomes a common practice.

Outlook

For over four decades, EOS has been one of the top causes of returns for semiconductor devices and systems. The Industry Council has documented here an extensive study which enhances understanding of EOS and recommends many approaches to reduce EOS damage. This should be of great value in preventing EOS from becoming a catastrophic issue in the next generation of technologies involving even more consumer, medical, military, and automotive applications. It would be important to revisit the information presented here at a later date and conduct another industry wide survey to see how much impact this work has made. EOS *is* inherent in the application of electronic systems. Only through continuous learning and sharing of experiences can future risks be avoided.

Appendix A: EOS Survey Form

Below is the EOS Survey Form that was used to survey EOS experience in the electronics industry

Industry Survey on Electrical Overstress (EOS)

While significant progress has been made over the past decades in the design, handling and application of electromagnetic compatible (EMC) and ESD protected electronic devices, there has hardly been much progress in the minimization of electrical overstress (EOS) of such devices. The Industry Council has recognized this deficiency and has decided to write a White Paper on EOS in order to help the industry to understand the root causes of EOS and minimize EOS of electronic devices.

In order to help us with this White Paper, we would appreciate, if you could answer all questions according to your experience with EOS of electronic devices.

Note, square selection boxes □ allow multiple choices, whereas circular selection boxes ○ allow only a single choice. Your source data will remain anonymous.

Please return the completed survey to EOSsurvey@esdindustrycouncil.com latest by February 28, 2013.

1. Demographic Data

a. What market segments does your company address?

- ❑ Consumer
- ❑ Industrial
- ❑ Automotive
- ❑ Aerospace
- ❑ Military
- ❑ Medical
- ❑ Other: _____

b. What kind of products do you manufacture?

- ❑ Discrete electronic devices
- ❑ Integrated Circuits (ICs)
- ❑ Printed Circuit Boards (PCBs)
- ❑ Systems

Specific products: _____

c. How many electronic devices do you ship / assemble per year (approximate order of magnitude)? _____

2. EOS Failures

a. How do you classify a failure as "EOS"?

- ❑ Based on the physical failure signature
- ❑ Based on the real-world electrical stress that caused it
- ❑ Based on replicated electrical stress that causes the same failure
- ❑ Based on the absolute maximum ratings of the failing device
- ❑ Based on the real root cause
- ❑ Based on _____

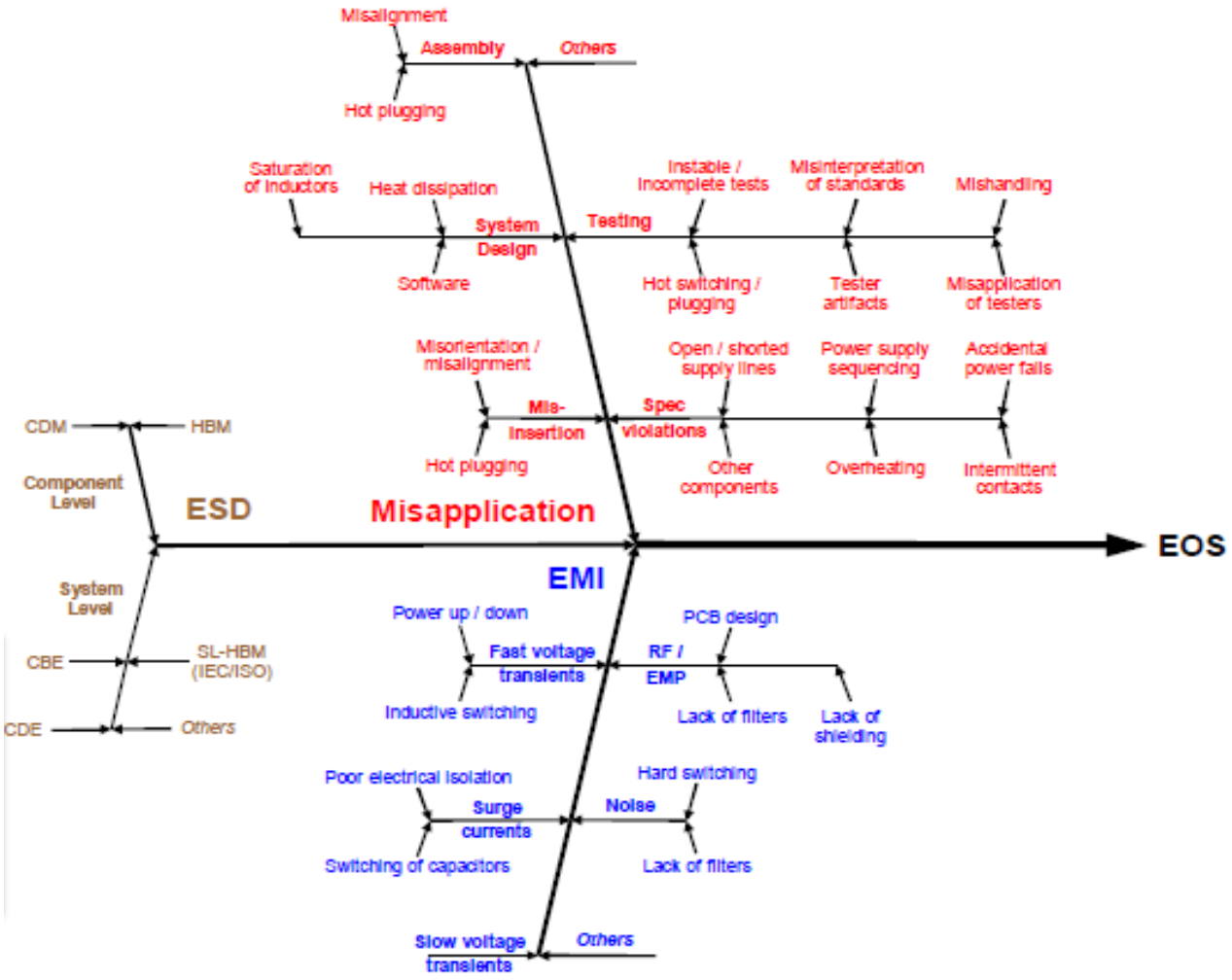
b. What type of failures do you classify as EOS?

- ❑ Permanent failures
- ❑ Temporary failures (e.g. functional failures)

3. Root Causes of Electrical Overstress (EOS)

In the broadest sense, typical EOS root causes can be grouped as shown in the fishbone diagram below into:

- Electrostatic discharge (ESD) events (e.g. HBM, CDM, CBE, CDE and lightning)
- Electromagnetic interference (EMI) issues (e.g. inductive switching, noise, EMP, etc.)
- Misapplications (e.g. misinsertion, power supply sequencing, etc.)
- Unknown root causes



According to the fishbone diagram above:

a. What is the rate of EOS failures in the number of *total* failures in your company? _____ %

b. What is the rate of EOS in the number of *electrical* failures in your company? ____ %

c. How does your company categorize the aforementioned cause of EOS failures?

ESD: ____ % EMI: ____ % Misapplication: ____ % Unknown: ____ %

d. Where do EOS failures experienced by your company typically occur? Device Manufacturer: ____ % Supplier: ____ % Assembly: ____ % Field: ____ %

e. What are the top 5 *specific* EOS root causes in your company (e.g. inductive switching, hot plugging, etc.)?

1) _____

2) _____
3) _____
4) _____
5) _____

f. What is the confidence level in your root cause diagnosis (100% = absolutely sure)?

_____ %

4. EOS Case Studies

The Industry Council wants to collect EOS case studies including EOS root causes or electrical stress (ES) events, ES transfers (injection method), ES characteristics, the occurrence of ES causing EOS, failure characteristics and how the problem was solved (or could have been solved). We are asking for your help to provide information on detailed EOS case studies. Please use the table below (or an extra sheet) to add your information as shown in the examples. If you do not have all the details, just fill in what you have.

	ES Characteristics				ES Occurrence		Failure	
EOS Cause / ES Event	ES Transfer	Duration	Energy	Primary ES	Application	Permanence	Failure Rate	Corrective Action
Hot plugging	Power lines	unknown	unknown	Energy	System repair	Permanent	500 dpm	First-mate-last-break (extended ground pin) connectors
Connector misorientation (reverse polarity)	Power lines	>1s	any	Current	User	Permanent	100 dpm	Fail-safe (asymmetrical) connectors
Noise	Radiation	≅ 5ns	n/a	Voltage	System manufacturer	Temporary	50 dpm	Filtering, shielding
CBE	Incidental contact	≅ 10ns	≅ 50µJ	Current	System manufacturer	Permanent	20 dpm	Discharge control

If you cannot provide any information on EOS case studies, please let us know why.

- ❑ We have no EOS problems
- ❑ We have no systematic documentation (e.g. database, failure reports, etc.)
- ❑ Information on EOS failures is company confidential
- ❑ Other reason:

5. Impact of EOS failures

a. How important is the reduction of EOS failures in your company?

- ○ Very important
- ○ Important
- ○ Neutral
- ○ Hardly important
- ○ Not important

b. When does your company start to worry about EOS failures? (For example, above a certain PPM level, at a certain pareto level of total failures, or a cost / time level, etc.).

6. Failure Reports

a. Are the failure reports (8D reports) of device manufacturers helpful? –

- ○ Yes
- ○ No

b. What information is missing or should be improved in failure reports (8D reports)?

c. When your company returns a failed device, does your company provide information on the conditions that caused the failure in order to improve the root cause diagnosis and correction?

- ○ Yes
- ○ Maybe
- ○ Don't know
- ○ Hardly

○ No

7. EOS Minimization

a. What is the most effective way to minimize EOS problems?

- ❑ Address the root cause
- ❑ Address the effect
- ❑ Avoid the electrical stress
- ❑ Increase the robustness of the electronic device
- ❑ Other: _____

b. What is your rate of solved EOS problems? ____ %

8. Absolute Maximum Ratings (AMR)

a. Do you provide AMR in your datasheets?

- ○ Yes
- ○ No

b. Are AMR important for your application?

- ○ Yes
- ○ No

c. What AMR information is missing or should be improved?

9. Further Remarks

Appendix B: The Dwyer Curve and EOS Damage at a Temperature Threshold

Tim Maloney, Intel Corporation

B.0 Background and 1-Dimensional Heat Flow

A great many studies of EOS, as in the preceding chapters (e.g., Figure 34 of Chapter 5) and in recent publications [1-3], include plotting of constant power-to-failure vs. time, usually on a log-log scale. The resulting curve is often called the Dwyer curve, following work such as in [4, 5]. In the late 1980s and early 1990s, the various features of the Dwyer curve were worked out and explained analytically, and the concepts were also applied to HBM and HBM-like pulses such as exponential and double-exponential [5, 6].

The starting point of most of these Dwyer curve discussions was the well-known Wunsch-Bell treatment [7] of a rectangular-pulsed heat source on an infinite heat sink, with heat flow in one dimension. In the Wunsch-Bell (W-B) model, failure occurs when the surface temperature crosses a threshold value, with the result that power-to-failure goes inversely as the square root of the pulse width. This of course is a descending straight line on a log-log plot, with a slope of half a decade per decade. For a typical semiconductor device, the W-B section will be a large part of the descending part of its Dwyer curve, but will not describe short or long times. At very short times, a discernible adiabatic section (power-to-failure goes as $1/\tau$ instead of $1/\sqrt{\tau}$) is common because of, e.g., bulk heating of surface metal. For longer times, the power-to-failure typically will flatten out and reach a steady state, owing to heat sinks and ultimate three-dimensional heat flow to give a constant thermal resistance.

The Dwyer curve is seen often enough that it could use some form of concise parametric characterization, so that Dwyer curves for various devices could easily be compared through those key parameters and so that a complete curve can be fit to a few measured points. If possible, we would like to express the entire Dwyer curve through a simple approximate analytical model, say with two parameters, easily deduced from experimental results, which uniquely place the curve on a log-log plot with considerable accuracy. We shall do this, and break new ground in this appendix. The concepts are not difficult, but do extend slightly beyond the analytic concepts developed some time ago [4-6]. It is possible that the arrival in the 1990s of better and more accessible computer tools (e.g., finite element modeling or FEM) drew attention away from analytic approximations because of their ability to supply nearly exact solutions for specific cases, and to simulate effects that are much harder to examine with simplified models. Nonetheless, simplified analytic models help to organize data, gain insight into the results, more efficiently allocate resources for full computer simulation, and also check simulation programs against known limiting cases. In that spirit, we extend and generalize the Wunsch-Bell picture to develop a complete simplified fit to the Dwyer curve.

B.1 Heat Flow as an RC Transmission Line

As pointed out in a 2013 IRPS paper [8] as well as in many other references, the one-dimensional (1-D) heat flow equation [9] is the same differential equation as for an RC electrical transmission line, namely $\frac{\partial^2 V}{\partial x^2} = RC\frac{\partial V}{\partial t}$. (1)

Temperature T is analogous to voltage V; 1/K per unit area (thermal conductivity K in W/cm-°C) is like resistance per unit length R; and $\rho C_p = C_v$ or volume heat capacity times unit area (ρ in gm/cm^3 and C_p in J/gm-°C) is like capacitance per unit length C. Accordingly, we aim to use various 1-D RC transmission line models along with lumped RC elements to solve a generalized heat flow problem to describe the Dwyer curve. We will analogize units as follows:

Volts→°C, temperature (usually a ΔT from room T)
Amps →Watts
Coulombs → Joules
Ohms →thermal impedance °C/W
Farads →Joules/°C

Distributed R-C heat flow paths will be represented by t-line segments having characteristic impedance Z_0 and propagation constant γ as from standard texts on RLGC lines, where for us, G=L=0 [10]:

$$Z_0 = \sqrt{\frac{R}{sC}} = \frac{1}{\sqrt{sK\rho C_p}} \qquad (2a)$$

$$\gamma = \sqrt{RCs} = \sqrt{\frac{s\rho C_p}{K}} \qquad (2b)$$

Note that these quantities depend on complex frequency s = σ+jω. The thermal impedance and impulse response of a semi-infinite solid (silicon, for example), would simply be Z_0 (scaled by area), and its temperature response to a step function heat source I_0/s amounts to finding a Laplace Transform of $s^{-3/2}$, proportional to $t^{1/2}$ [11]. This is the famous Wunsch-Bell result [7]. Their results were obtained with "effective" material parameters over a given temperature range, and of course that remains a consideration when working with these linearized models.

The reasoning in the above paragraph invokes the notion of an Ohm's Law in the s-domain that is common in circuit analysis, V(s) = I(s)Z(s), where Z(s) is the impedance (Eq. 2a in the W-B semi-infinite case). The same concepts apply to temperature, heat flow, and thermal impedance because the equations are the same. Also, the convolution theorem [12] tells us that the time domain is described through V(t) = I(t)⊗Z(t), where ⊗ is the convolution operator and Z(t) the thermal impulse response, and inverse Laplace transform of Z(s). Once we have the thermal impedance Z(t) or Z(s), it should be straightforward to apply a constant power source (current), i.e., integrate Z(t), to find where failure threshold temperature (voltage) is reached.

B.2 Thermal Impedance and the Jacobi Theta4 Function

In the 1-D view, the Dwyer curve is most simply captured by terminating the transmission line at a certain length *l* by a short, as shown in Figure B1. At long times, we expect a pure resistor V=IR and therefore the flat part of the Dwyer curve. For this tanh (shorted) line, the exponential form of tanh expands as 1/(1-x) into the numerator to form a single series,

$$Z_{in} = Z_0 \tanh(\gamma l) = \frac{1}{\sqrt{K\rho C_p s}}\left(1 - 2e^{-2B\sqrt{s}} + 2e^{-4B\sqrt{s}} - 2e^{-6B\sqrt{s}} + \cdots\right) \quad , (3)$$

$B = \sqrt{\frac{\rho C_p}{K}} l$. This inverts into the time domain [11], term by term, to form

$$Z_{in} = Z_{\tanh}(t) = \frac{1}{\sqrt{\pi K\rho C_p l}}\left(1 - 2e^{-B^2/t} + 2e^{-4B^2/t} - 2e^{-9B^2/t} + \cdots\right) \quad . (4)$$

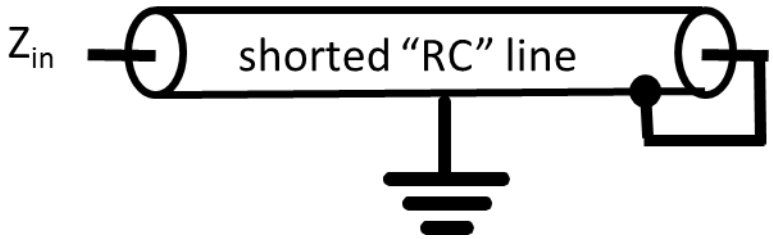


Figure B1: Transmission line terminated by a short (perfect heat sink), for a simplified model to be associated with the Dwyer curve

The series (4) is a form of the Jacobi Theta4 function [13], with ϑ_4 parameter z=0 and

$$q = \exp(-\frac{B^2}{t}) = \exp(-\frac{\rho C_p}{Kt} l^2),$$

$$\vartheta_4(q) = 1 + 2\sum_{k=1}^{\infty} (-1)^k q^{k^2} \quad . (5)$$

We are interested in 0<q<1, as 0<t<∞. Therefore,

$$Z_{\tanh}(t) = \frac{1}{\rho C_p l} \frac{\vartheta_4(\exp(-(t^*/t))}{\sqrt{\pi t / t^*}} \quad , (6)$$

$t^* = B^2 = \frac{\rho C_p}{K} l^2$, a time constant. The ϑ_4 function and the normalized impulse response function for $Z_{tanh}(t)$ are shown in Figure B2. Since the q series (5) converges slowly, it is best to compute values with the following series [13], which converges in a few terms to within parts per billion and beyond for our range of interest:

$$\vartheta_4(q) = 2\sqrt{\frac{\pi}{-\ln(q)}}\exp\left[\frac{\pi^2}{4\ln(q)}\right]\sum_{k=0}^{\infty}\exp\left[\frac{k(k+1)\pi^2}{\ln(q)}\right]. \quad (7a)$$

But note that since q=exp(-(t*/t)), ln(q) = -t*/t. Thus

$$Z_{in} = Z_{\tanh}(t) = \frac{2l}{t^* K}\exp\left[-\frac{\pi^2 t}{4t^*}\right]\sum_{k=0}^{\infty}\exp\left[-\frac{k(k+1)\pi^2 t}{t^*}\right]. \quad (7b)$$

The expected steady-state value of thermal resistance, *l*/K, results from integrating over time and finding the infinite sum. The same result is found by inspection if the problem is posed in $Z_{in}=\tanh(\sqrt{s})/\sqrt{s}$ form and $\tanh(\sqrt{s})$ computed as an infinite product ([11], 4.5.68-69). Z_{in} is reducible to a pole-zero expansion in s—for s=0, $Z_{in}(s)=l/K$. Heaviside inversion of this expression also gives Eq. (7b) in time domain, after negotiating a number of infinite products.

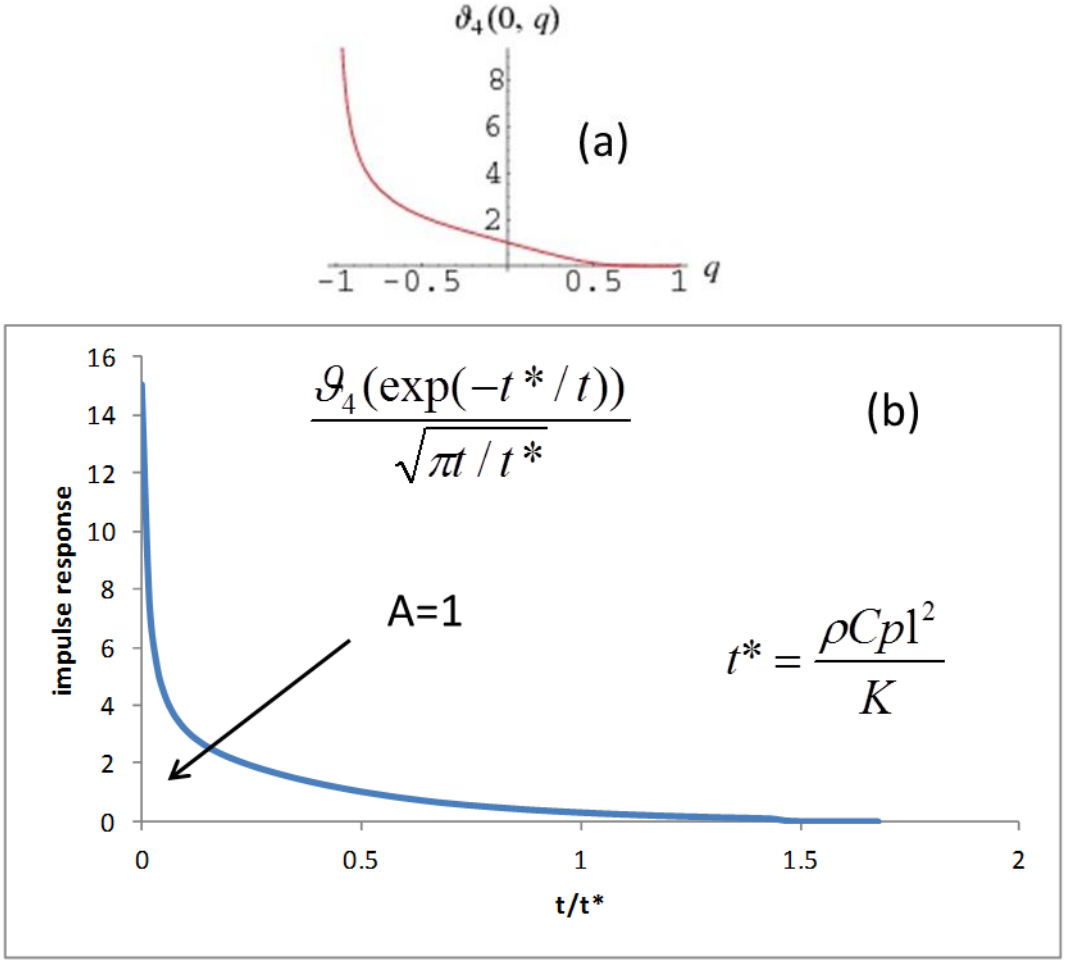


Figure B2: (a) Plot of Jacobi Theta4 (ϑ_4) function [13]. (b) Normalized impulse response from Z(t) of shorted t-line, Eq. (6).

The surface temperature is computed by convolving Figure B2b (times applicable constants) with the power flow function to obtain the entire T(t) waveform. The rectangular pulse of the Dwyer curve is particularly simple, with peak temperature resulting from integrating thermal $Z(t) = Z_{th}(t)$, or

$$T(t_0) = P_0 \int_0^{t_0} Z_{th}(t)dt \quad . (8)$$

Thus

$$P_{crit}(t_0) = \frac{T_{crit}}{\int_0^{t_0} Z_{th}(t)dt} \quad . (9)$$

This means that a measured Dwyer curve $P_{crit}(t)$ leads right back to an impulse response $Z_{th}(t)$ through the reciprocal of its slope:

$$Z_{th}(t_0) = \frac{d}{dt}\left[\frac{T_{crit}}{P_{crit}(t)}\right]_{t=t_0} . (10)$$

This sort of reasoning is also implicit in much earlier work, as with the Duhamel formula cited in [5, 6]. But let us continue with our aim of using the thermal impulse response to solve for the Dwyer curve.

B.3 The Analytic Dwyer Curve Approximation

For infinitely long line length *l*, Z_{in} reduces to $Z_0(s)$, Eq. (2a), and we are back to the W-B case, where $Z(t) = Z_{th}(t)$ goes as $t^{-1/2}$. Also the area A (Figure B2b) becomes infinite and thus there is no flattening of the power-time curve. Refs [4-6] are concerned with convolution of the W-B Z(t) with the exponential P(t) power functions associated with HBM and similar tests (e.g., ISO 7637-2 [3]), in which case a SOA can be identified by plotting peak power vs. characteristic time, usually the exponential decay constant τ. The SOA boundary for peak power for a pure exponential ends up being almost a factor of two above the (Eq. (9)) rectangular pulse W-B curve—an exact answer can be worked out as in [5] because the convolution integral is Dawson's integral [14]. The peak power vs. time curve is $2x_0$=1.848… above the rectangular pulse curve, where x_0 is the Dawson integral turning point [5], $D(x_0)$=Dmax.

We now show, in Figure B3a, the integral of the normalized impulse response Z(t) from Figure B2b, i.e., the step response to a constant power step. This function is

$$F(t) = \int_0^t \frac{\vartheta_4(\exp(-t^*/t_0))}{\sqrt{\pi t_0 / t^*}} dt_0 \qquad (11)$$

which converges to 1 as shown. The delay time is characterized by the area in the upper left hand corner and is found to be, in normalized terms, 1/3. Thus a CAD measurement of step power response can be fit to this kind of impedance function by setting final temperature to 1 (giving a

scaling factor Z_0 from T_{final}/P_0) and multiplying the time delay area, as shown, by 3 to give t*. The Elmore Delay [15] of 1/3 for this function represents the first moment of the impulse response, or

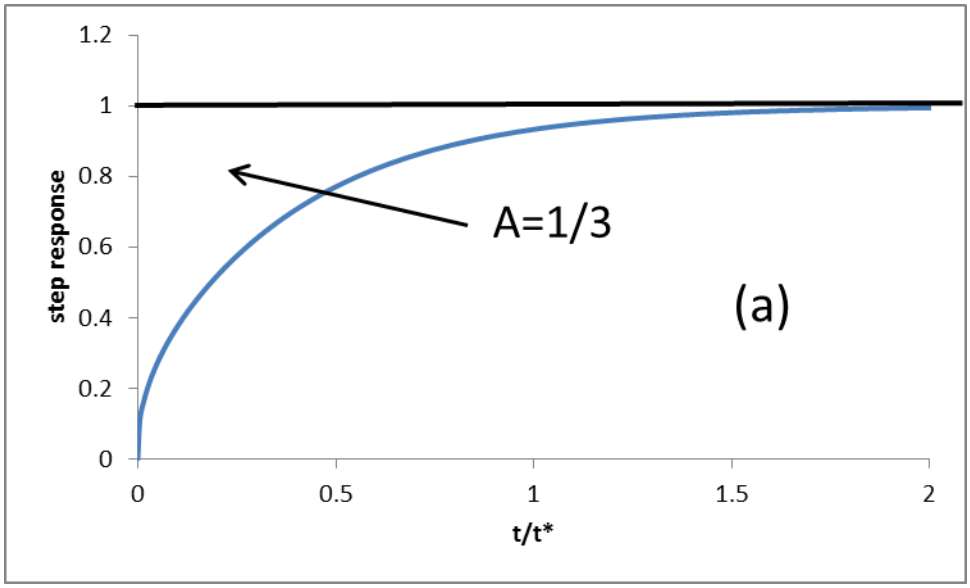
$$m_1 = \int_0^\infty \sqrt{\frac{t}{\pi t^*}}\vartheta_4(\exp(-t^*/t)dt = \frac{1}{3}. \qquad (12)$$

The relationship is most easily proven by going back to the s-domain expression for the shorted line Z(s) as in (3) and expanding tanh for the normalized function to give

$$Z_{norm}(s) = \frac{1}{\sqrt{st^*}}\tanh\left[\sqrt{t^* s}\right] = 1 - \frac{1}{3}t^* s + \cdots \qquad (13)$$

with (minus) the s-coefficient being the delay time [15].

For finite line length, we have a heat sink, A=1 as in Figure B2b, and thus for long enough time, t/t* will be large, the integral of Z(t) will be unchanging and thus the Dwyer power-time curve will be flat. This is of course the V=IR (or $T_{crit}=P_{crit}\cdot Z_{th}$) type of condition. The transition from falling slope to flat power-time curve is captured by the integral of Z(t) out to various times. This is shown on a semilog plot in Figure B3.



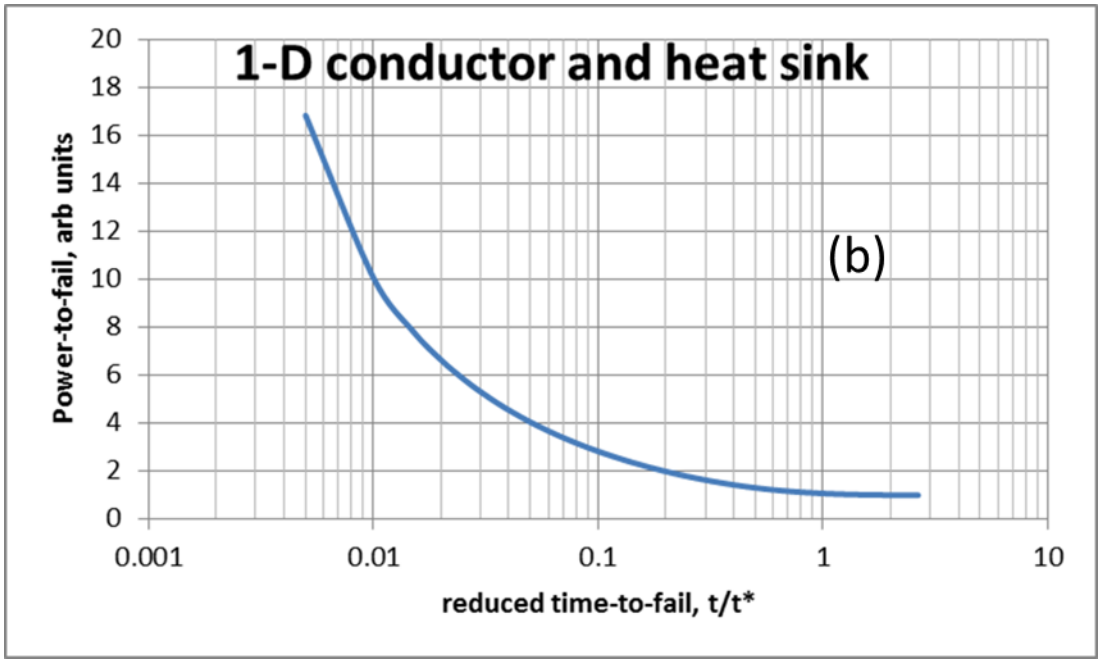


Figure B3: (a) Integrated normalized Z(t) (step response) from Figure B2b, showing convergence to 1 and Elmore Delay [15] of t*/3. (b) Semilog plot of Normalized Dwyer Curve based on 1D Heat Flow Model of Figure B1.

The normalized curve converges to 1 on the order of time constant t*, as expected. It is not clear how to parameterize the plot, but the curve resembles other semilog Dwyer curve plots, as in [1]. A more enlightening view is seen in Figure B4, a log-log plot of the same data. While the W-B limit is at very short times, there is also a long section in the middle of the descending curve, more than a decade in time, which can be fit with a line and extrapolated to intercept the steady-state $P_{crit}(\infty)$ value at about t=0.79t*. Now we have what we need to fit the entire curve, t*(a function of length, defined following Eq. (6)) and the steady state value $P_{crit}(\infty)$. Then in accordance with Eq. (9),

$$P_{crit}(t) = \frac{P_{crit}(\infty)}{\int_0^t \frac{\vartheta_4(\exp(-(t^*/t))}{\sqrt{\pi t / t^*}}\, dt} \qquad (14)$$

and we have the entire Dwyer curve, with $\vartheta_4(q)$ defined by (7). Everything is normalized to the final value of P_{crit}, but we can go to Eq. (6) and the definition of t* to deduce T_{crit} from estimates of length *l* and thermal conductivity K, or some similar interrelationship. We certainly have $Z_{th}(t)$ to within a scaling constant once we have t*.

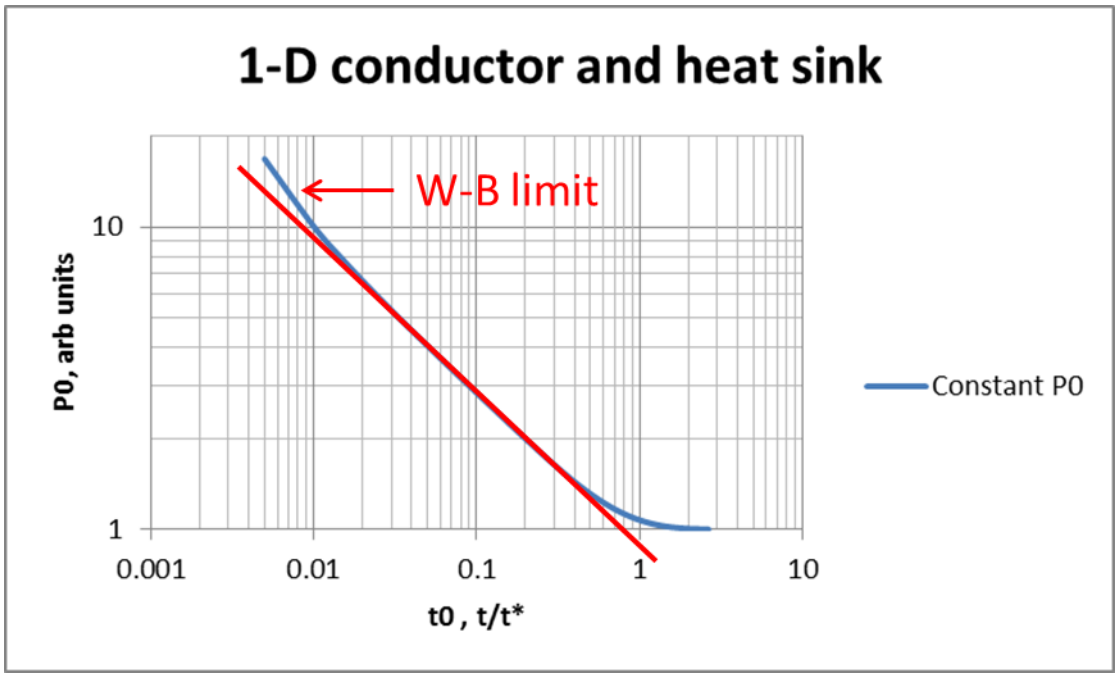


Figure B4: Log-log plot of normalized Dwyer curve, or Eq. (9), showing power law in the mid-section, extrapolated to t=0.79t*. This is how to extract a characteristic time t* from plotted data.

Now we can return to the exponential power function, with decay constant τ (tau), and compare its peak power curve P_{pk} to the Dwyer constant power curve with power P_0 and pulse length t_0. We take the derived $Z_{th}(t)$ function as in Eq. (6) and convolve with the exponential power function, point by point, to give the upper curve in Figure B5. Inasmuch as the exponential power calculation reduces to the Dawson integral in the W-B limit of $Z_{th}(t)$, as discussed earlier, we expect the upper curve in Figure B5 to be $2x_0$=1.848… above the lower curve on the left-hand end. We do see that, but the trend continues up to around τ=t* and P_{pk} begins the long process of converging to P_0 for τ>>t*.

We can now apply these methods to some actual Dwyer curve device data as in [1], shown in Figure B6. The transition region between the two groups of data (covering almost two orders of magnitude of time) can now be filled in because we have a complete "reasonable" Dwyer curve after using the curve fits shown to arrive at P_{final}=7.062W and t*=110.14 μsec. The power law section is extrapolated to P_{final} (taken at 1msec) and the intercept point is t=0.79t* as noted above.

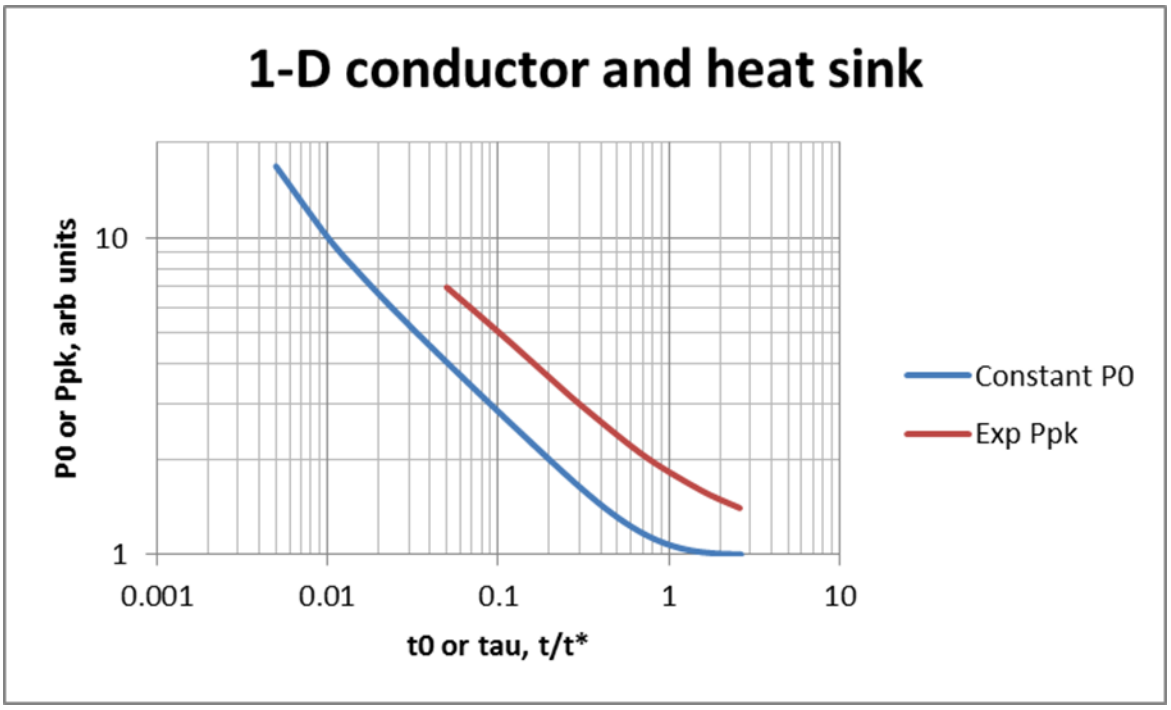


Figure B5. Constant power P_0 Dwyer curve (blue) vs. pulse length t_0 compared with peak power P_{pk} exponential curve (red) vs. time constant τ, normalized to t*. Exponential curve calculated from convolution with Z(t) as in Eq. (6) and over most of its range is about $2x_0$=1.848… above the constant power curve as predicted by the Dawson integral.

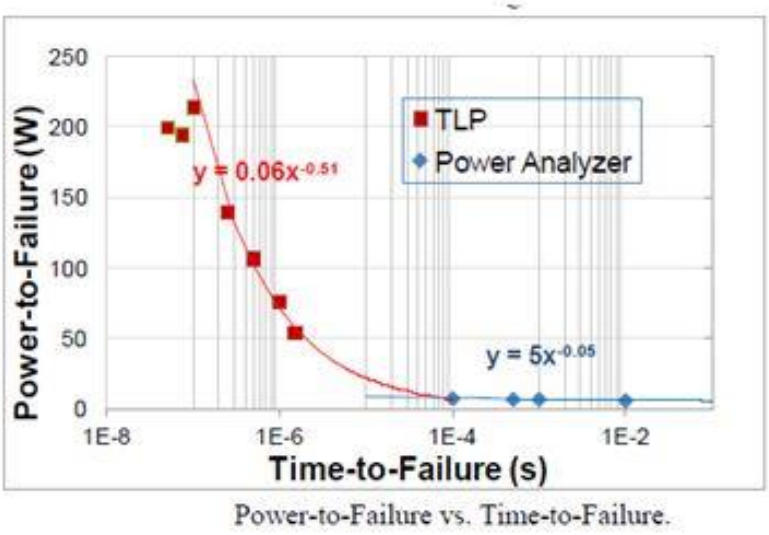


Figure B6: Dwyer curve device data as in Figure 12 of [1], taken with two different instruments.

The power law approximations from [1] as in Figure B6 are also pretty good, as we plot the Figure B6 Dwyer curve log-log in Figure B7. After extracting $Z_{th}(t)$ using Eq. (10), we convolve and plot the exponential power function (red) also, resembling Figure B5. The red curve in Figure B7 lies 1.75-1.95x above the blue curve in the sloped portion, generally as expected and in agreement with Figure B5.

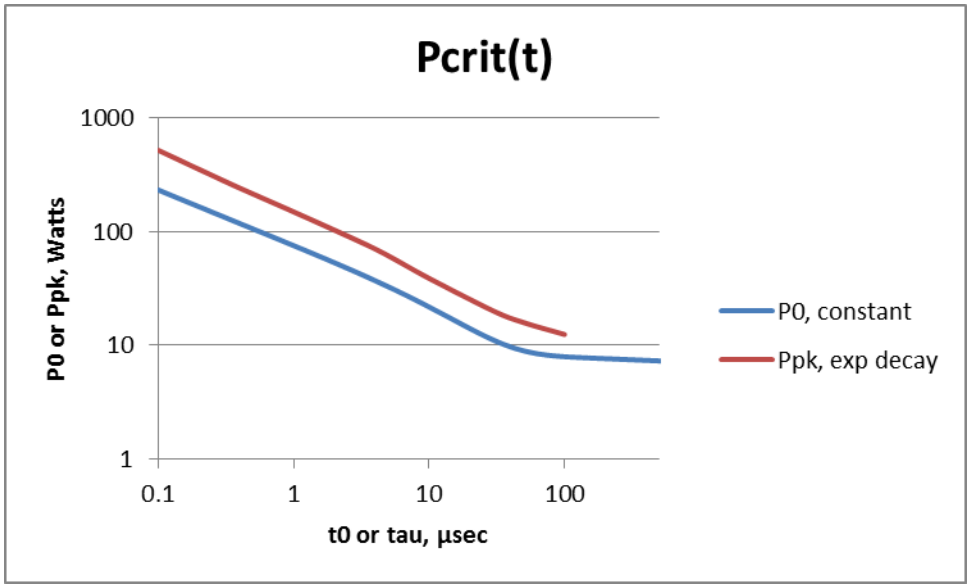


Figure B7: Dwyer curve (blue) plotted log-log from power laws in Figure B6 [1]. Result for exponential power function (red) lies 1.75-1.95x higher over most of its range, as expected.

B.4 Utility of the Dwyer Curve and Thermal Impedance Approximations

The 1-D heat flow model with perfect heat sink located by a characteristic time constant is of course an idealized way to look at the kind of heat flow effects that allow the $Z_{th}(t)$ integral to converge and the Dwyer curve to flatten out. Many of these effects relate to the ultimate 3-D nature of heat flow, whereby the flow out of a rectangular slab will at first seem one-dimensional (with W-B $t^{-1/2}$ impulse response), then if its aspect ratio is large there will be apparent 2-D heat flow (t^{-1} impulse response). But on a long enough time scale, every heat source is a 3-D point source, with $t^{-3/2}$ impulse response (the rule of thumb is $t^{-1/2}$ per dimension [9]) even into an infinite slab. The step response of these thermal impedances, i.e., the time integrals, will not converge for one ($t^{1/2}$) or two (ln t) dimensions, but will converge for three dimensions ($t^{-1/2}$) once the point source effect takes over the time dependence. In the 1-D approximation, this is modeled as an "effective" heat sink, located to produce an appropriate time constant. Heat sinks, although imperfect, are expected in the real case as well, because heat diffuses further and further with distance. Still, the approximation of 1-D with heat sink works remarkably well as a way to capture the various parts of the Dwyer curve with meaningful parameters.

These concepts can even be used to speed up computer calculations of heat flow. Suppose you have a 2-D transistor heat flow model that is computationally much faster than a complete 3-D model. The latter may better represent the real case but is slower. A few simulations could help equip the more interactive 2-D model with a well-located artificial heat sink that better represents the 3-D effects that are felt at longer times. The effects can be bounded so that having the artificial sink is "no better than" having actual 3-D behavior, yet close. In this way, the iterative exploratory process (involving a human agent learning things from both 2-D and 3-D models) could be enhanced.

References

[1] T. Smedes, Y. Christoforou, and S. Zhao, “Characterization Methods to Replicate EOS Fails”, Proc. EOS/ESD Symposium, vol. 36, pp. 384-392, 2014.

[2] A. Kamdem, P. Martin, J.-L. Lefebvre, F. Berthet, B. Domenges, and P. Guillot, “Electrical Overstress Robustness and Test Method for ICs”, Proc. EOS/ESD Symposium, vol. 36, pp. 393-399, 2014.

[3] F. Magrini and M. Mayerhofer, “Advanced Wunsch-Bell Based Application for Automotive Pulse Robustness Siaing”, Proc. EOS/ESD Symposium, vol. 36, pp. 400-407, 2014.

[4] V. M. Dwyer, A. J. Franklin, and D. S. Campbell, "Thermal Failure in Semiconductor Devices", Solid State Electronics, vol. 33. pp. 553-560, 1990.

[5] V. M. Dwyer, A. J. Franklin, and D. S. Campbell, “Electrostatic Discharge Thermal Failure in Semiconductor Devices”, IEEE Trans. Elec. Dev., vol. 37, no. 11, pp. 2381-87, Nov. 1990.

[6] D. G. Pierce, W. Shiley, B. D. Mulcahy, K. E. Wagner, and M. Wunder, "Electrical overstress testing of a 756K UVEPROM to rectangular and double exponential pulses," Proc. EOS/ESD Symp., vol. 10, pp. 137-146, 1988.

[7] D. C. Wunsch and R. R. Bell, "Determination of Threshold Failure Levels of Semiconductor Diodes and Transistors Due to Pulse Voltages," IEEE Trans. Nucl. Sci., NS-15, pp. 244-259, 1968.

[8] T. J. Maloney, L. Jiang, S. S. Poon, K. B. Kolluru, and AKM Ahsan, "Achieving Electrothermal Stability in Interconnect Metal During ESD Pulses", 2013 Int'l Reliability Physics Symposium.

[9] H. S. Carslaw and J. C. Jaeger, *Conduction of Heat in Solids*, 2nd edition. Oxford, UK: Oxford University Press, 1959.

[10] S. Ramo, J. Whinnery, and T. Van Duzer, *Fields and Waves in Communication Electronics*. New York: John Wiley & Sons, 1965.

[11] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*. New York: Dover Publications, 1965. Laplace Transform tables are in Sec. 29.

[12] R. N. Bracewell, *The Fourier Transform and Its Applications*, New York: McGraw-Hill, 1965.

[13] Web article, http://functions.wolfram.com/EllipticFunctions/EllipticTheta4/.

[14] Web article, http://mathworld.wolfram.com/DawsonsIntegral.html.

[15] W.C. Elmore, “The Transient Analysis of Damped Linear Networks With Particular Regard to Wideband Amplifiers”, J. Appl. Phys. Vol. 19(1), pp. 55-63 (1948).

Appendix C: Frequently Asked Questions

Q1: When I send a suspected EOS damaged unit back to a supplier after failure, how can I increase the supplier's chances of determining the cause?

Answer: Customers can help significantly in the determination of root cause for a failure by including as much background information on the history of the unit as possible. Chapter 6 of the white paper provides customer guidance for a list of information that will help suppliers determine cause when customers submit a suspected EOS damaged unit to a supplier for analysis.

Q2: Why can't I just send a suspected EOS damaged unit back to a supplier and expect the supplier to tell me why it failed?

Answer: Without a good description of the operational background history of a device, a supplier may only be able to describe the actual physical symptoms of the failure. This can be especially true for EOS units that are heavily damaged. The background history helps the supplier first understand if the physical symptoms of failure that they uncover make sense based on the device history. In addition, the background history may help the supplier disregard some collateral damage symptoms so that the analysis can focus on the most likely root cause. The information described in Sections 6.2 and 6.4 are typically quite useful for planning and conducting an analysis; but suppliers may also request additional background information after initiation of the investigation based on the symptoms they observe.

Q3: With technology scaling advances, wouldn't you expect much more sensitivity to EOS returns?

Answer: This is intuitively correct, but tracking of FA returns to EOS has so far shown no large correlation. However, we caution that with further advances in technology, including even thinner gate oxides, AMR levels will be reduced resulting in a likely impact on returns if AMR levels are not well understood and adhered to. The industry would do well to track this into the future.

Q4: Why would there be a higher chance of EOS returns with 4 kV or 6 kV protection designs? Has this really been observed?

Answer: First, the Industry Council data between 500 V to 2 kV HBM has shown no correlation to the rate of EOS returns (See JEP155). However, there has been some observation that IC designs with exceptionally high levels of HBM seem to show a relatively more frequent number of EOS returns. What could be the cause for this? Generally, high HBM protection involves SCR devices which can trigger much more easily with any type of voltage spikes, substrate injection, etc. So this could be one possible explanation. Further, low HBM protection diodes had higher resistance and did not draw much unexpected current, i.e. are less sensitive to trigger events.

Q5: Do soft fails also belong to EOS related fails?

Answer: Soft fails are non-permanent functional fails of a system such as unintended power-down, loss of memory data or unexpected reset. While these can be caused by various electrical stress conditions which also lead to physical EOS damage, they are commonly not considered EOS related due to the missing physical damage signature. However, in the case of a soft fail, an assessment of compliance with absolute maximum rating should be performed and, if needed, environmental and

electrical conditions should be adjusted. Yet soft fails can occur even if the AMR threshold of an IC component is not exceeded due to the complex interaction between electrical pulse and system.

Q6: Is the fishbone diagram of EOS root causes complete?

Answer: The fishbone diagram is not exhaustive and there are many more root causes which can lead to an EOS. The purpose of the fishbone diagram is to show the basic categories of EOS root causes. This should help in the analysis of EOS damage. Vice versa, the categories can be used as a guide for consideration and implementation of appropriate countermeasures in the early system design phase and in the control of the system environment and operation later on.

Q7: Can better "designed-in" ESD robustness improve EOS?

Answer: While excessive ESD is considered as a cause of EOS damage, enhanced ESD protection is not correlated to higher EOS tolerance. ESD protection might not be active under EOS conditions. In spite of this, enhanced ESD protection might even lead to lower thresholds for certain types of EOS damage, for example, latch-up damage for low holding snapback protection devices.

Q8: What are some of the on-die or within package clues from IC damage that could result more from an EOS event than an ESD event?

Answer: Damage from component level ESD events tends to be localized to small areas of the circuit, and generally does not include more extensive heat-related package damage. Damage from system level ESD or EOS events (whether externally generated, misapplication or process related) tends to involve larger circuit areas, tends to be visible in more than one location (often along one or more paths), tends to involve circuitry not normally damaged in first failing component level ESD events, and can involve silicon melt as well as package melt damage.

Q9: Where in the system (supply chain, manufacturing, and field) have ICs been most reported with suspected EOS damage?

Answer: Most (over 80%) of companies reporting in the survey of suspected EOS damage reported experiencing this damage either in system assembly or in the field. However, electrically induced physical damage (EIPD) damage which can be suspected to be EOS can occur from other causes than direct transients which violate the AMR and may involve test escapes, process aberrations or unintended unanticipated design related issues at different points in the process which can cause EIPD to occur nearly anywhere in the product development flow. It is important for customer and supplier to consider all options in the case of suspected EOS damage and keep the investigations continuing until a root cause can be identified and a corrective action determined.

Q10: Is there a disconnect between the perceived importance of resolving EOS issues and company reports on EOS?

Answer: Yes. Over 85% of companies surveyed reported EOS as being "important" or "very important" to their company, yet over half of the companies surveyed reported that their company EOS issues are not communicated to supplier or customer due to various issues (see survey questions 4 and 5a in Chapter 2). This is a major disconnect that White Paper 4 addresses through careful examination of EOS case studies in Chapter 5 and communication of proper definitions of EOS and AMR in Chapter 3.

Q11: Shouldn't the FA report of a device suspected of damage due to overstress <u>conclude</u> that the damage was due to overstress and indicate where the overstress occurred? Wouldn't that help resolve the issue?

Answer: No! The FA report, whether generated from a supplier or an independent failure analysis facility, should take every effort to reveal the extent of failed areas and thermal damage, and could give an opinion regarding what type of electrical stress may have occurred, but cannot conclude where the failure occurred. Only after cooperation and discussion with the customer can any specific conclusions regarding the specific location of where the overstress occurred be drawn. The report must be communicated to the customer and both supplier and customer must work together to share information about different parts of their process, testing, assembly, application and operation which can then be used to develop investigations and tests to help replicate the failure. The 8D report format is an increasingly preferred technique to gather information and direct investigations to help find root causes and determine corrective actions.

Revision History

Revision	Changes	Date of Release
1.0	Initial Release	April, 2016
1.1	Logo update	April, 2016
1.2	-Logo update -Updated to align with JEDEC version of document, this resulted in: -Minor grammer changes -Changes to Terms and Definitions -Description of region B which resulted in changes to the Executive Summary and Chapter 3, Section 3.1 and Chapter 7, Section 7.2.3 -Clarification added to Executive Summary and Chapter 3, Section 3.1 clarifying that some qualification stresses such as ESD and Latch-up are expected to run evaluations which exceed AMR.	August, 2016