

JEDEC PUBLICATION

System Level ESD Part II: Implementation of Effective ESD Robust Designs

JEP162A

(Revision of JEP162, January 2013)

SEPTEMBER 2019

JEDEC SOLID STATE TECHNOLOGY ASSOCIATION



NOTICE

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

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

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

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

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

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

Published by
©JEDEC Solid State Technology Association 2019
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2107

This document may be downloaded free of charge; however JEDEC retains the copyright on this material. By downloading this file the individual agrees not to charge for or resell the resulting material.

PRICE: Contact JEDEC

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

PLEASE!

DON'T VIOLATE
THE
LAW!

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

For information, contact:

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

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

System Level ESD

Part II: Implementation of Effective ESD Robust Designs

Contents

	Page
Introduction	iii
1.1 Overview	iii
1.2 Understanding Component to System ESD	iv
1.3 Communication and Strategy	v
1.4 Implementation of Advanced Tools	v
1.5 Impact from the Technology Roadmap	vi
1.6 Conclusions	vi
1 Scope.....	1
2 References.....	1
3 Terms and Definitions.....	6
4 Background and Outline	11
4.1 History of the Industry Council on ESD Target Levels	11
4.1 History of the Industry Council on ESD Target Levels (cont'd).....	12
4.2 JEP162 (White Paper 3 Part II): Summary of Clauses/Annexes.....	12
4.2 JEP162 (White Paper 3 Part II): Summary of Clauses/Annexes (cont'd)	13
4.2 JEP162 (White Paper 3 Part II): Summary of Clauses/Annexes (cont'd)	14
5 Overview of ESD Stressing and System Response.....	15
5.1 Presently Used Stress Tests for ESD.....	15
5.1 Presently Used Stress Tests for ESD (cont'd).....	16
5.2 Definitions.....	16
5.2 Definitions (cont'd).....	17
5.3 Coupling of ESD into Systems and Circuits	17
5.4 Troubleshooting to Determine the Cause of Failures.....	21
5.5 New Technologies for Determining Root Cause of Failures.....	21
5.6 Summary	24
6 State-of-the-Art ESD/EMI Co-design.....	24
Introduction	24
6.1 The Basics.....	25
6.2 Advanced System ESD Protection Methods	33
6.3 Comprehensive Co-Design Methodologies.....	38
6.4 Conclusion	39
7 Reference Methodologies for IC/System Protection Co-Design.....	40
Introduction	40
7.1 Approaches – Categories.....	42
7.2 Examples	52
8 Standard Model and Analytical Tool Needs To Support SEED	58
Introduction	58
8.1 Component Characterization and Model Requirements to Support SEED Category 1.....	59
8.2 Component Characterization and Model Requirements to Support SEED Category 2.....	68
8.3 System Characterization and Model Requirements to Support SEED Category 3	69
8.4 Conclusion	78
9 Summary and Conclusions.....	79
Introduction	79
9.1 Overview of ESD Stressing and System Response - Clause 5.....	79
9.2 State-of-the-Art ESD/EMI Co-Design - Clause 6.....	79
9.3 Reference Methodologies for IC/System - Clause 7	81
9.4 Standard Model and Analytical Tool Needs to Support SEED - Clause 8.....	82
9.5 Application Specific Information on System ESD Related Tests and Their Targets – Annex A.....	82
9.6 Technology Roadmap and Direction – Annex B	83

9.7 Outlook.....	84
Annex A: Application Specific Information on System ESD related Tests and their Targets	85
Introduction	85
A.1 System Tests and Targets of Mobile Phones	85
A.2 System Tests and Targets of Automotive Electronic Components	87
A.3 System Tests and Targets of Computing Devices.....	89
A.4 System Tests and Targets of Medical Electronic Components	90
A.5 System Tests and Targets of Avionic Components.....	91
A.6 System Tests and Targets of Consumer Electronic Devices	92
A.7 Applicability of System-Efficient ESD Design (SEED).....	93
Annex B: Technology Roadmap and Direction.....	95
Introduction	95
B.1 Roadmap for ICs: Microprocessors	96
B.2 Roadmap for Automotive Applications	98
B.3 Roadmap for IC Package and Applications	99
B.4 Advances in Board and Assembly Technologies	101
B.5 Optical Interconnects	104
B.6 Polymer Applications.....	104
B.7 Future Compatibility to IEC Protection Requirements	106
Annex C: Fast and Slow ESD Stress (High and Low Frequency Spectrum).....	109
Discussion.....	109
C.1 Some Words on ESD Debugging.....	112
Annex D: Review of JEP161 (White Paper 3 Part I).....	113
D.1 JEP161 Clause 4: Purpose and Introduction	113
D.2 JEP161 Clause 5: Test Methods and Their Field of Application	113
D.3 JEP161 Clause 6: Proven System Level Fails.....	115
D.4 JEP161 Clause 7: OEM System Level ESD Needs and Expectations	116
D.5 JEP161 Clause 8: Lack of Correlation between HBM/CDM and IEC 61000-4-2	117
D.6 JEP161 Clause 9: Relationship between IC Protection Design and System Robustness	118
D.7 JEP161 Clause 10: Summary, Conclusions and Outlook.....	120
Annex E: Frequently Asked Questions.....	121
Annex F: Differences between revisions	127

Foreword

This document is the second of two Electrostatic Discharge (ESD) Industry Council white papers dealing with System Level ESD (Part I is JEP161).

In JEP161, the misconceptions common in the understanding of system level ESD between supplier and original equipment manufacturer (OEM) were identified, and a novel ESD component / system co-design approach called system efficient ESD design (SEED) was described. The SEED approach is a comprehensive ESD design strategy for system interfaces to prevent hard (permanent) failures. In JEP162 we expand this comprehensive analysis of system ESD understanding to categorize all known system ESD failure types, and describe new detection techniques, models, and improvements in design for system robustness. JEP162 also expands this SEED co-design approach to include additional hard / soft failure cases internal to the system.

JEP162A begins with an overview of system ESD stress application methods and introduces new system diagnosis methods to detect weak ESD failure areas leading to hard or soft failures, and provides a “cost vs. performance vs. robustness” analysis of present-day state-of-the-art electromagnetic compatibility (EMC)/electromagnetic interference (EMI) design prevention methods that have been developed to prevent system level ESD failure. It follows with an expansion of SEED failure classifications to cover a combination of hard (permanent) and/or soft (resettable) system failures and stresses which could cause these errors, and describes cases where the SEED co-design approach can be expanded to provide additional benefits to system ESD design. System design simulation tools are described in the context of their potential improvements to simulating system level ESD stress and failure modes. Application-specific industry system ESD test methods are then described in the context of their ability to reveal hard and soft failure modes from actual system deployment. Finally, a technology roadmap of the system design components is described, including IC technology and related circuit speeds, automotive electronics, packaging technology, system / board interconnect technology and ESD protection materials, illustrating continuing challenges for system ESD design improvement.

Introduction

I.1 Overview

JEP162A, while establishing the complex nature of System Level ESD, proposes that an **efficient ESD design can only be achieved when the interaction of the various components under ESD conditions are analyzed at the system level**. This objective requires an appropriate characterization of the components and a methodology to assess the entire system using simulation data. This is applicable to system failures of different categories (such as hard, soft, and electromagnetic interference (EMI)). This type of systematic approach is long overdue and represents an advanced design approach which replaces the misconception, as discussed in detail in JEP161, that a system will be sufficiently robust if all components exceed a certain ESD level.

In the first step, a method for categorizing the failure types has been introduced. An advanced characterization and simulation approach is discussed through examples. However, a full design flow cannot be established without **a common effort across the electronic industry involving IC suppliers, suppliers of discrete protection components and original equipment manufacturers (OEMs) as well as tool vendors**. This paper identifies existing tools with both simulations and scanning techniques that are applicable for this purpose and calls out fields for further development.

I.1 Overview (cont'd)

Equally important is the notion that **efficient system ESD design can ideally be achieved by improved communication between the IC supplier, the OEM and the system builder**. As technologies advance even further, and as systems become more complex under various applications, this shared responsibility is expected to gradually shift more towards system design expertise.

I.2 Understanding Component to System ESD

Towards achieving the goals mentioned above, it is first important to decouple the component ESD requirements from system level ESD design. JEP155 and JEP157 established that component electrostatic discharge (ESD) levels can be safely reduced to practical levels with basic ESD control methods that are mandatory in every production area. We have also established that these ESD target levels enable fabrication of integrated circuits (ICs) with on-time delivery (in billions of units) for electronic systems in consumer applications with high circuit performance. The general perception has been that component ESD (for example, human body model (HBM)) is a prerequisite for good system level ESD robustness. But this misconception once again needs to be clarified, as shown below in Figure 1, **system level ESD and component ESD are not correlated with each other.**

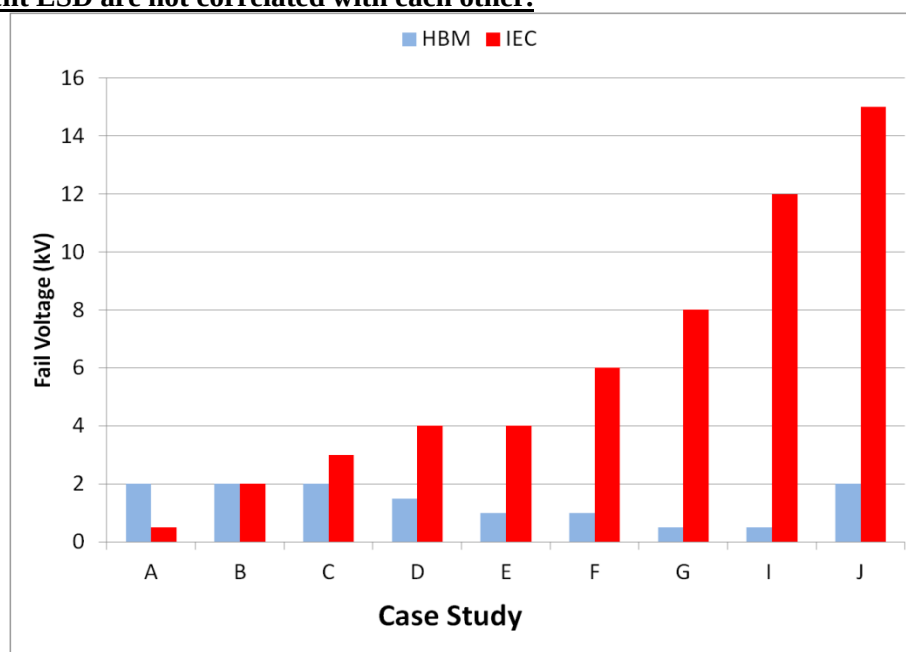


Figure 1 — Comparison of IC level and system level ESD failure threshold of various systems (A-J) showing that HBM protection is not related to System level ESD robustness

In fact, at the system level, ESD robustness is a much more complex issue requiring a deeper understanding to address the ESD protection requirements for electronic systems such as laptops, cell phones, printers and home computers. These system complexities come about as a result of protecting the external interfaces, such as a universal serial bus (USB), to the outside world. Such systems, after encountering the more severe ESD pulses defined by the IEC standard, can lead to hard or soft failures. As introduced in JEP161, the basic version of system-efficient ESD design (SEED) addresses **hard failures** related to IC pins with a direct external interface, **soft failures**, which are more frequently reported, are challenging to understand and overcome. In this latter case, addressing soft failures requires an extension of the SEED approach to other failure mechanisms that include latch-up and EMI effects. In this document, the steps to categorize the different failure mechanisms, and the appropriate characterization and simulation methodologies, are identified through various forms of **Advanced SEED**.

I.3 Communication and Strategy

This white paper documents a rigorous approach to describing **the challenges related to all categories of system level ESD failures** that can arise from energy injection due to the IEC contact pulse stress, as well as from electromagnetic compatibility (EMC) and EMI effects. To classify these fails and to provide a common terminology, three categories of fails have been introduced:

- SEED Category 1 (physical damage due to pulse energy)
- SEED Category 2 (damage or interference of function due to transient latch-up)
- SEED Category 3 (interference of function by noise or bursts on supply net and signal lines)

Understanding these different categories of failures is an important part of addressing the appropriate solutions. Thus, one main objective is to close the existing communication gap between OEMs and IC providers by involving the expertise of both OEMs and system design experts. As a result, the completion of this second phase of White Paper 3 required the participation and contributions from world class experts on the art of system level ESD phenomena and protection techniques.

One of the challenges which remains elusive is the trade-off between cost, performance, robustness, and time-to-market. This white paper also addresses these issues, bringing forth a dialogue between the IC supplier, customer, and the system designer.

I.4 Implementation of Advanced Tools

JEP162 specifically covers in detail **an overview of system ESD stress application methods, system diagnostic techniques to detect hard or soft failures, and the application of tools for susceptibility scanning**. For example, as illustrated in Figure 2, these types of advanced tools can be used to differentiate the characteristics of products and enable proper system protection methodology.

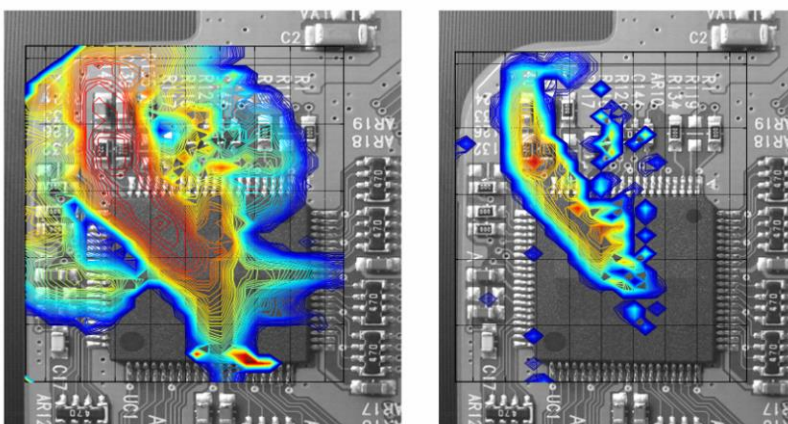


Figure 2 — Susceptibility scanning using pulse techniques on Product A (left) and Product B (right)
(Courtesy of Amber Precision Instruments)

I.4 Implementation of Advanced Tools (cont'd)

Along the lines of communication and interaction, IC suppliers and system designers can share their knowledge of tools and their applications. For example, suppliers would provide a single definition, high quality model of their input/output (IO). Then OEMs would use analytical tools to integrate the IC's IO models into their system models for system level stress analysis. These tools will not reach their full potential unless the data they collect can be used within the standard design flow for an electronic system. For these to be effective, model files such as input/output buffer information specification (IBIS) and simulation programs with integrated circuit emphasis (SPICE), which describe the electrical properties of components, need to be enhanced to describe component behavior in the ESD range. The general framework for such modeling has been defined through IEC 61433-6 and the detailed models around the integrated circuit itself, such as discussed above, are currently in definition based on an industry wide investigation performed by ESDA WG26 on system level ESD modeling. Suppliers of components, ranging from integrated circuits to ESD protection devices, also need to characterize their products in the appropriate ESD range.

I.5 Impact from the Technology Roadmap

Finally, we bring into focus that IC technology and related circuit speeds will increasingly have an impact on system designs. This roadmap will cover market segments ranging from information technology (IT), communications, automotive electronics, IC package technology development to advances in board and assembly technologies. **The cost of ESD must be considered along with all development and innovation; the industry must decide who should bear the cost of ESD design and its pressure on production schedules and time to market**

System level ESD will continue to be a challenge in the future. The dilemma of meeting technology demands for speed and performance will inevitably require either the development of more effective shielding or innovation of novel on-board protection solutions.

I.6 Conclusions

In summary, this white paper has pointed out the necessary framework required for comprehensive improvement in the first time success rate of ESD robust system designs. A number of helpful tools and techniques already exist. However, standardization between IC suppliers, PCB protection device suppliers and system designers requires common models, common methods and compatible simulation tools in order to meet the goal of better ESD design capability. **None of this will occur without a great deal of communication between EDA tool vendors, component suppliers and system designers.**

Finally, this document has provided a major step forward in identifying and understanding the technical issues. An important message to remember is that **the current focus on component ESD performance must shift towards improving system level ESD performance. That is, while minimum component ESD levels provide for safe component handling, the bulk of future research and development efforts should be directed towards system level ESD to reach a day when a high first pass success rate in system level ESD design is straightforward.**

System Level ESD

Part II: Implementation of Effective ESD Robust Designs

(From JEDEC BoD Ballot JCB-12-66 and JCB-19-23, formulated under the cognizance of the JC-14.3 Subcommittee on Wafer-Level Reliability.)

1 Scope

This white paper consolidates industry-wide knowledge and experience on the tools and methods used to address failures of printed circuit boards (PCBs) which occur as a result of IEC 61000-4-2 system-level ESD stressing. These include both hard and soft failures, but more emphasis is placed on soft failures from all the observed and anticipated failures and failure scenarios. The methodology is a consistent characterization approach which applies to both IC interfaces and discrete PCB components.

2 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 www.esda.org 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 www.esda.org or JEDEC publication JEP157, "Recommended ESD-CDM Target Levels", www.jedec.org
- [3] JEITA document EDR-4709, 2012
- [4] Industry Council on ESD Target Levels, "White Paper 3 System Level ESD Part I: Common Misconceptions and Recommended Basic Approaches," December 2010, at www.esda.org or JEDEC publication JEP161, "System Level ESD Part I: Common Misconceptions and Recommended Basic Approaches", www.jedec.org
- [5] IEC 61000-4-2, 'Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test', Ed. 2.0, 2008.
- [6] Jayong Koo; Qing Cai; Kai Wang; Maas, J.; Takahashi, T.; Martwick, A.; Pommerenke, D., "Correlation Between EUT Failure Levels and ESD Generator Parameters", IEEE Trans. EMC. Vol.50, Issue 4, Nov. 2008 pp. 794 - 801
- [7] Anderson, W., Eppes, D, Beebe, S. "Metal and Silicon Burnout Failures from CDM ESD Testing", Proc. EOS/ES Symp., Sept. 2009, pp. 2A.6-1 - 2A.6-8.
- [8] Voldman, Steven H., "ESD Failure Mechanisms and Models", John Wiley & Sons, Ltd, 2009, pp. 35-37.
- [9] Muchaidze, G., Jayong Koo, Qing Cai, Tun Li, Lijun Han, Martwick, A., Kai Wang, Jin Min, Drewniak, J.L., Pommerenke, D., "Susceptibility Scanning as a Failure Analysis Tool for System-Level Electrostatic Discharge (ESD) Problems", IEEE Trans. EMC, May 2008, Vol 50, No. 2, pp. 268-276
- [10] Kai Wang; Jayong Koo; Muchaidze, G.; Pommerenke, D.J. "ESD susceptibility characterization of an EUT by using 3D ESD scanning system", IEEE Int. Symp. on EMC, 8-12 Aug. 2005, pp. 350-355, Vol.2
- [11] Zhen Li, David Pommerenke, "Electrostatic Discharge Induced Upset Probability Database for Transient Field Coupling to Integrated Circuits", presently under review (2012) IEEE Transactions on EMC, contact davidjp@mst.edu

2 References (cont'd)

- [12] Maheshwari, P.; Tianqi Li; Jong-Sung Lee; Byong-Su Seol; Sedigh, S.; Pommerenke, D.; ,
“Software-Based Analysis of the Effects of Electrostatic Discharge on Embedded Systems”,
Computer Software and Applications Conference (COMPSAC), 2011 IEEE 35th Annual , pp. 436-
441, 18-22 July 2011
- [13] Maheshwari, P.; Byong-Su Seol; Jong-Sung Lee; Jae-Deok Lim; Sedigh, S.; Pommerenke, D.; ,
"Software-Based Instrumentation for Localization of Faults Caused by Electrostatic Discharge,"
High-Assurance Systems Engineering (HASE), 2011 IEEE 13th International Symposium, pp.333-
339, Nov. 2011
- [14] Laasch, Ingo et al, “Latent Damage due to multiple ESD Discharges,” EOS/ESD Symposium, 2009,
pp. 1-6
- [15] Hua, Vanessa, “Sparks over static: An age-old problem still vexes makers of tech devices,” San
Francisco Chronicle, August 27, 2001
- [16] Frei, S.; Wu, W.; Hilger, U.; Edenhofer, J.; Stecher, M.: “Packaging and Handling Test according to
ISO 10605: How comparable are tests with different ESD generators?”, ESD-Forum 2007, Munich,
Germany, 2007
- [17] D. Johnson, H. Gossner; “Study of System ESD Co-design of a realistic Mobile Board”,
Proceedings of 33rd EOS/ESD Symposium (2011), pp. 360-369
- [18] G. Notermans, S. Bychikhin, D. Pogany, D. Johnsson, D. Maksimovic, “HMM–TLP correlation for
system-efficient ESD design”, Microelectronics Reliability, 2011
- [19] zur Nieden, F.; Scheier, S.; Arndt, B.; Frei, S.: “Gefährdung von integrierten Schaltungen durch
Überkopplungen zwischen Leiterbahnen auf Platinen“, ESD-Forum 2011, Munich, Germany, 2011
- [20] S. Poon, T. Maloney; “Shielded Cable Discharge Induces Current on Interior Signal Lines“, Proc.
29th EOS/ESD Symposium (2007), pp. 311-317
- [21] JEDEC Standard “IC Latch-Up Test”; JESD78D; November 2011.
- [22] Ming-Dou Ker, Sheng-Fu Hsu. “Physical Mechanism and Device Simulation on Transient-Induced
Latch-up in CMOS ICs Under System-Level ESD Test” IEEE Transactions on Electron Devices,
vol. 52, no. 8, August 2005, pp. 1821-1831
- [23] Farzan Farbiz and Elyse Rosenbaum. “Understanding Transient Latch-up Hazards and the Impact of
Guard Rings”, International Reliability Physics Symposium, 2010, pp. 466-473
- [24] K. Domanski, B. Poltorak, S. Bargstaedt-Franke, W. Stadler, W. Bala. “Physical fundamentals of
external transient latch-up and corrective actions”, Microelectronics Reliability 46 (2006) pp. 689–
701
- [25] Brodbeck, T.; Stadler, W.; Baumann, C.; Esmark, K.; Domanski, K.; “Triggering of transient latch-
up (TLU) by system level ESD” EOS/ESD Symposium 2010 pp. 1-10
- [26] I. Morgan, C. Hatchard, M. Mahanpour, “Transient Latch-Up Using an Improved Bi-polar Trigger”,
Proc. 21st EOS/ESD Symposium (1999), pp. 190-202
- [27] S. Bargstaedt-Franke a, W. Stadler, K. Esmark, M. Streibl, K. Domanski, H. Gieser, H. Wolf, W.
Bala. “Transient latch-up: experimental analysis and device simulation”, Microelectronics
Reliability 45 (2005) pp. 297–304
- [28] Wang, Dening; Marum, Steve; Kemper, Wolfgang; McLain, David; “System event triggered latch-
up in IC chips: test issues and chip level protection design”, EOS/ESD Symposium 2006, pp. 1-7
- [29] D. Bonferta, H. Giesera, H. Wolfa, M. Frankb, A. Konradb, J. Schulzc, “Transient-Induced latch-up
test setup for Wafer-Level and Package Level”, Microelectronics Reliability 46 (2006) pp. 1629–
1633
- [30] R. Llido a, J. Gomez a, V. Goubier a, N. Froidevaux a, L. Dufayard a, G. Haller a, V. Pouget b, D.
Lewis b. “Photoelectric Laser Stimulation applied to Latch-Up phenomenon and localization of
parasitic transistors in an industrial failure analysis laboratory”, Microelectronics Reliability 2011

2 References (cont'd)

- [31] J. Quincke, "Novel Test Structures for the Investigation of the Efficiency of Guard rings Used for IO-Latch-up Prevention", ICMTS 1990, pp. 35-39
- [32] S. Liao, C. Niou, K. Chien, A. Guo, W. Dong, C. Huang, "New Observance and Analysis of Various Guard-Ring Structures on Latch-Up Hardness by Elackside Photo Emission Image", IRPS 2003, pp. 92-98
- [33] Ming-Dou Ker, Wen-Yu Lo, and Chung-Yu Wu, "New Experimental Methodology to Extract Compact Layout Rules for Latch-up Prevention in Bulk CMOS ICs", Custom Integrated Circuits, Proceedings of the IEE 1999, pp. 143-146
- [34] Ming-Dou Ker, Member, IEEE, and Chung-Yu Wu, Member, IEEE, "Modeling the Positive-Feedback Regenerative Process of CMOS Latch-up by a Positive Transient Pole Method-Part I: Theoretical Derivation", IEEE Transactions on Electron Devices, vol. 42, no. 6, June 1995, pp. 1149-1155
- [35] D. Estreich, R. Dutton, "Modeling Latch-Up in CMOS Integrated Circuits", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. cad-1, no. 4, October 1982, pp. 157-162
- [36] Felipe Coyotl Mixcoatl, Alfonso Torres Jacome, "Latch-up prevention by using guard ring structures in a 0.8 μm bulk CMOS process", 2004
- [37] B. L. Gregory and B. D. Shafer, "Latch-up in CMOS Integrated Circuits" IEEE Transactions on Nuclear Science, Vol 20, 1973, pp. 293-299
- [38] Gensuke Goto, Hiromasa Takahishi and Tetsuo Nakamura, "Latch-Up Immunity Against Noise Pulses in a CMOS Double Well Structure", 1983 Electron Devices Meeting, pp. 168-171
- [39] K. Domanski, M. Heer, K. Esmark, D. Pogany, W. Stadler, E. Gornik. "External (transient) Latch-up Phenomenon Investigated by Optical Mapping (TIM) Technique", EOS/ESD Symposium 2007, pp. 6A.3-1 – 6A.3-10
- [40] Ming-Dou Ker, Senior Member, IEEE, and Sheng-Fu Hsu, Student Member, IEEE, "Component-Level Measurement for Transient-Induced Latch-up in CMOS ICs Under System-Level ESD Considerations", IEEE Transactions On Device And Materials Reliability, vol. 6, no. 3, September 2006, pp. 461-472
- [41] M. Kelly, "Developing a Transient Induced Latch-up Standard for Testing Integrated Circuits", Proc. 21st EOS/ESD Symp. (1999), pp. 178–189
- [42] Xiao, J.; Pommerenke, D.; Drewniak, J. L.; Shumiya, H.; Maeshima, J.; Yamada, T.; Araki, K.; "Model of Secondary ESD for a Portable Electronic Product", IEEE Trans. EMC, Oct. 2011, pp. 1-10
- [43] Wei Huang; Dunnihoo, J.; Pommerenke, D.; "Effects of TVS integration on system level ESD robustness.", EOS/ESD Symposium 2010, pp. 1-6
- [44] Jayong Koo, Qing Cai, Muchaidze, G. Martwick, A.Kai Wang, Pommerenke, D, "Frequency-Domain Measurement Method for the Analysis of ESD Generators and Coupling", IEEE Trans. EMC, Aug. 2007, Vol. 49, No.3, pp. 504-511
- [45] Liu, D.; Nandy, A.; Zhou, F.; Huang, W.; Xiao, J.; Seol, B.; Lee, J.; Fan, J.; Pommerenke, D. "Full-Wave Simulation of an Electrostatic Discharge Generator Discharging in Air-Discharge Mode Into a Product", IEEE Trans. EMC, Vol.99, 2010, pp. 28-37
- [46] Maheshwari, Pratik; Seol, Byong-Su; Lee, Jong-Sung; Lim, Jae-Deok; Sedigh, Sahra; Pommerenke, David; "Software-Based Instrumentation for Localization of Faults Caused by Electrostatic Discharge", 13th Ins. Symposium on High-Assurance Systems Engineering (HASE), 2011, pp. 333-339
- [47] Weiying Li, Yu Tian, Linpeng Wei, Chai Gill, Weil Mao, Chuanzheng Wang, "A Scalable Verilog-A Modeling Method for ESD Protection Device", 2010 EOS/ESD symposium, pp. 1-10

2 References (cont'd)

- [48] Patrice Besse, Frédéric Lafon, Nicolas Monnereau, Fabrice Caignet, Jean-Philippe Laine, Alain Salles, Sophie Rigour, Marise Bafleur, Nicolas Nolhier, David Trémouilles, "ESD system level characterization and modeling methods applied to a LIN transceiver", 2011 EOS/ESD Symposium, pp. 329-337
- [49] T. Smedes, J. van Zwol, G. de Raad, T. Brodbeck, H. Wolf, "Relations between system level ESD and (vf) TLP", EOS/ESD Symposium 2006. pp. 136-143
- [50] Patrice Besse, Jean-Philippe Laine, Alain Salles, Mike Baird, "Correlation Between System Level and TLP tests Applied to Stand-alone ESD Protections and Commercial products", 2010 EOS/ESD Symposium, pp. 151-156
- [51] Yiqun Cao, Ulrich Glaser, Joost Willemsen, Filippo Magrini, Michael Mayerhofer, Stephan Frei, Matthias Stecher, "ESD Simulation with Wunsch-Bell based Behavior Modeling Methodology", 2011 EOS/ESD Symposium, pp. 187-195
- [52] K. Wang et al., "Numerical modeling of electrostatic discharge generators," in IEEE Trans. Electromagnetic Compatibility, vol. 45, no. 2, pp. 258- 271, May 2003
- [53] S. Caniggia and F. Maradei, "Circuit and Numerical Modeling of Electrostatic Discharge Generators," IEEE Trans. Ind. Appl., vol. 42, no. 6, pp. 1350-1357, Nov. 2006
- [54] R. Mertens et al., "A Flexible Simulation Model for System Level ESD Stresses with Application to ESD Design and Troubleshooting," in Proceedings of EOS/ESD Symposium, 2012, pp. 1-6
- [55] N. Monnereau; F. Caignet; N. Nolhier; D. Trémouilles, "Investigating the probability of susceptibility failure within ESD system level consideration", EOS/ESD Symposium 2011, September 11-16, 2011, pp. 1-6.
- [56] N. Monnereau; F. Caignet; N. Nolhier; D. Trémouilles; M. Bafleur, "Behavioral-modeling methodology to predict electrostatic-discharge susceptibility failures at system level: an IBIS improvement", Electromagnetic Compatibility (EMC) Europe, York, UK, September 26-30, 2011, pp. 457-463.
- [57] K. Muhonen, J. Dunnihoo, E. Grund, N. Peachey, A. Brankov, "Failure Detection with HMM Waveforms", EOS/ESD Symposium 2009, 5B.3, pp. 1-9.
- [58] Jiang Xiao, D. Pommerenke, Fan Zhou, J. L. Drewniak, H. Shumiya, T. Yamada, K. Araki, "Model for ESD LCD upset of a portable product", 2010 IEEE International Symposium on Electromagnetic Compatibility (EMC), pp. 354-358
- [59] zur Nieden, F; private communication
- [60] T. W. Chen, T. J. Maloney, and B. Chou, "Detecting E and H Fields with Microstrip Transmission Lines", 2008 EMC Symposium, August 2008, pp. 1-6
- [61] T. J. Maloney, A. Martwick, K. Wang, "Measuring Electric and Magnetic Field", US Patent application, filed Aug. 30, 2007. Issued as US Patent 7,750,629, July 6, 2010.
- [62] C. E. Baum, E. L. Breen, J. C. Giles, J. O'Neill, and G. D. Sower, "Sensors for Electromagnetic Pulse Measurements Both Inside and Away from Nuclear Source Regions", IEEE Trans. Electromagnetic Compatibility, Vol. EMC-20, No. 1, pp. 22-35, February 1978.
- [63] CFR 47 §xx.xx -- http://www.access.gpo.gov/nara/cfr/waisidx_02/47cfrv2_02.html
- [64] EN 300 xxx -- <http://www.etsi.org/WebSite/Standards/Standard.aspx>
- [65] EN 301 xxx -- <http://www.etsi.org/WebSite/Standards/Standard.aspx>
- [66] EN 55020 -- <http://www.etsi.org/WebSite/Standards/Standard.aspx>
- [67] EN 55024 -- <http://www.etsi.org/WebSite/Standards/Standard.aspx>
- [68] TS 25.xxx -- <http://www.etsi.org/WebSite/Standards/Standard.aspx>
- [69] TS 36.xxx -- <http://www.etsi.org/WebSite/Standards/Standard.aspx>
- [70] TS 51 xxx -- <http://www.etsi.org/WebSite/Standards/Standard.aspx>
- [71] TS 151 xxx -- <http://www.etsi.org/WebSite/Standards/Standard.aspx>
- [72] GBT 22450.1-2008 - - <http://www.ptsnet.cn/> (Chinese only)

2 References (cont'd)

- [73] YDT 1592.1 - <http://www.ptsn.net.cn/> (Chinese only)
- [74] PTCRB NAPRD.03 -- <http://www.ptcrb.com/>
- [75] ETS 300 342-1 -- <http://www.etsi.org/WebSite/Standards/Standard.aspx>
- [76] ISO 10605 -- http://www.iso.org/iso/iso_catalogue.htm
- [77] IEC 61967 -- <http://webstore.iec.ch/>
- [78] IEC 62132 -- <http://webstore.iec.ch/>
- [79] ISO 7637 -- http://www.iso.org/iso/iso_catalogue.htm
- [80] ISO 16750-2 -- http://www.iso.org/iso/iso_catalogue.htm
- [81] CISPR 12 -- <http://webstore.iec.ch/>
- [82] CISPR 25 / EN55025 -- <http://webstore.iec.ch/>
- [83] ISO 11451 -- http://www.iso.org/iso/iso_catalogue.htm
- [84] ISO 11452 -- http://www.iso.org/iso/iso_catalogue.htm
- [85] SAE J1113 -- <http://standards.sae.org/>
- [86] AEC Q100 -- <http://www.aecouncil.com/AECDocuments.html>
- [87] Ford Motor Company, EMC Design Guide for Printed Circuit Boards, Engineering Specification ES-3U5T-1B257-AA,
<http://www.fordemc.com/docs/download/EMC%20Design%20Guide%20for%20PCB.pdf>
- [88] Ford Motor Company, Electromagnetic Compatibility Specification for Electrical/Electronic Components and Subsystems, General Specification Electrical/Electronic, EMC-CS-2009.1,
http://www.fordemc.com/docs/download/EMC_CS_2009rev1.pdf
- [89] Audi, BMW, Daimler, Porsche, and Volkswagen, Hardware Requirements for LIN, CAN and FlexRay Interfaces in Automotive Applications, version 1.1, 2009.
- [90] CISPR 24:2010 -- <http://webstore.iec.ch/>
- [91] ISO 14971:2007 -- http://www.iso.org/iso/iso_catalogue.htm
- [92] 21 CFR 1000- 1299 -- <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm>
- [93] 21 CFR 1000.15 --
<http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?FR=1000.15>
- [94] EN/IEC 60601-1-2 -- <http://webstore.iec.ch/>
- [95] MDD 93/42/EEC -- <http://eur-lex.europa.eu/>
- [96] W. Kimmel and D.D. Gerke: "Exploring systems EMC in Medical Devices",
<http://www.eetimes.com/design/medical-design/4212205/Exploring-systems-EMC-in-medical-devices>
- [97] IEEE C62.41.1 – 2002 – <http://ieeexplore.ieee.org/>
- [98] IEEE C62.41.2 – 2002 – <http://ieeexplore.ieee.org/>
- [99] IEEE C62.45 – 2002 – <http://ieeexplore.ieee.org/>
- [100] MIL-STD-461 -- <http://assist.daps.dla.mil/quicksearch/>
- [101] RTCA DO-160 -- <http://www.rtca.org/downloads/>
- [102] EUROCAE ED-14 -- <http://www.eurocae.net/>
- [103] MIL-STD-464 -- <http://assist.daps.dla.mil/quicksearch/>
- [104] CISPR 13 -- <http://webstore.iec.ch/>
- [105] Tai-Ho Wang; Wen-Hao Ho; Lin-Chien Chen; "On-Chip system ESD protection design for STN LCD drivers", EOS/ESD Symposium, 2005, 8-16 Sept. 2005, pp. 1 - 7.
- [106] Pavey, LD.; Kerr, J.; "ESD simulation and cure: a case study", ESD and ESD Counter Measures IEE Colloquium on 28 Mar 1995, pp. 1 - 4.
- [107] Ming-Dou Ker; Cheng-Cheng Yen; "Investigation and Design of On-Chip Power-Rail ESD Clamp Circuits Without Suffering Latch-up-Like Failure During System-Level ESD Test" IEEE Journal Solid State Circuits, Nov. 2008, Vol.42, pp. 2533-2545

2 References (cont'd)

- [108] Ming-Dou Ker, Wan-Yen Lin¹, Cheng-Cheng Yen¹, Che-Ming Yang, Tung-Yang Chen, Shih-Fan Chen, "Protection Design Against System-Level ESD Transient Disturbance on Display Panels", 2010 Asia-Pacific International Symposium on Electromagnetic Compatibility, April 12 - 16, 2010, Beijing, China, pp. 438-411
- [109] Cheng-Cheng Yen; Wan-Yen Lin; Ming-Dou Ker; Che-Ming Yang; Shih-Fan Chen; Tung-Yang Chen; "New transient detection circuit to detect ESD-induced disturbance for automatic recovery design in display panels", Design & Technology of Integrated Systems in Nanoscale Era (DTIS), 2011, pp. 1-4
- [110] J.Xiang, D. Pommerenke et.al. "Model for ESD LCD Upset of a Portable Product", IEEE International Symposium on EMC, 2010, pp. 354-358
- [111] S. Bertonnaud, C. Duvvury; "IEC System Level ESD Design for OMAP™ System", private communication (International ESD Workshop 2011, Lake Tahoe)
- [112] H. Gossner, C. Russ, J. Schneider, K. Schrufer, T. Schulz, C. Duvvury, R. Cleavelin, W. Xiong, "Unique ESD Failure Mechanism in a MuGFET Technology," IEDM Tech. Digest, pp. 101-106, 2006.
- [113] D. Edwards, "High Performance IC Package Design and Electrical Reliability," EOS/ESD Symposium Proceedings, 2003, pp. 1-7
- [114] David Miller, "Rationale and Challenges for Optical Interconnect to Electronic Chips," Proceedings of the IEEE, Vol. 88, No. 6, June 2000, pp. 728-749
- [115] M. Uusimaki and A. Renko, "A systematic Approach and comparison of different 3-D chip structures for electromagnetic compatibility" IEEE 0-7803-8443-1/04, 2004 IEEE International Symposium on EMC, pp. 734-739
- [116] Based on empirical evidence coupled to the German OEM requirements and through personal communication with M. Hell, Infineon Technologies
- [117] <http://www.esdforum.de/Files/Impact%20of%20Lowering%20the%20ICHBM%20Robustness.pdf>

3 Terms and Definitions

AAMI	Association for the Advancement of Medical Instrumentation
AC	alternating current
ADC	analog digital converter
AEC	Automotive Electronics Council
AMR	absolute maximum rating
ANSI	American National Standards Institute
ASIC	application specific integrated circuit
ASTM	American Society for Testing and Materials
ATE	automated test equipment
BCD	bipolar-CMOS-DMOS
BOM	bill of materials
CAD	computer aided design
CAN	controller area network
CBE	charged board event
CCL	capacitive coupled latch-up
CDE	cable discharge event
CDM	charged-device model

3 Terms and Definitions (cont'd)

CISPR	Comité International Spécial des Perturbations Radioélectriques
CMOS	complimentary metal-oxide-semiconductor
CMF	common mode filter
CRC	cyclic redundancy check
DC	direct current
DDR	double data rate
DIP	dual inline package
DMOS	double-diffused metal-oxide-semiconductor
DSP	digital signal processing
DVI	digital visual interface
DUT	device under test
ECU	electronic control unit
EDA	electronic design automation
EEPROM	electrically erasable programmable read only memory
EFT	electrical fast transients
EM	electromagnetic
EMMI	emission microscopy
EOS	electrical overstress
ESD	electrostatic discharge
ESDA	Electrostatic Discharge Association; ESD Association
ETSI	European Telecommunication Standards Institute
EUT	equipment under test
FB	ferrite bead
FDA	Food and Drug Administration
FET	field effect transistor
FFT	fast Fourier transform
GND	negative voltage supply in digital logic, neutral voltage supply in analog logic
GPIO	general purpose input/output
HBM	human body model
HDL	hardware description language
HDMI	high definition multimedia interface
HMM	human metal model
IBIS	input/output buffer information specification
IC	integrated circuit
ID	identification
IO	input/output
IEC	International Electrotechnical Commission
IR	infra-red
ISO	International Organization of Standards
IT	information technology
ITE	information technology equipment
I-V	current/voltage
JEDEC	JEDEC Solid State Technology Association
JEITA	Japan Electronics and Information Technology Industries Association
JTAG	joint test action group
LCD	liquid crystal display
LED	light emitting diode
LIN	local interconnect network

3 Terms and Definitions (cont'd)

MCM	multi-chip module
MDD	medical device directive
MEM	micro-electro-mechanical
MID	molded interconnection device
MM	machine model
OEM	original equipment manufacturer
ODM	original design manufacturer
OTP	one time programmable
PC	personal computer
PCB	printed circuit board
PCI	peripheral component interconnect
PHY	physical layer interface
PLL	phase lock loop
PN	p-type/n-type junction
PWB	printed wiring board
R2R	roll-to-roll
RAM	random access memory
RC	resistor capacitor network
RF	radio frequency
RLC	resistor inductor capacitor network
RTOS	real time operating system
RX	receiver
SAE	Society of Automotive Engineers
SAW	surface acoustical wave
SCR	silicon controlled rectifier
SERDES	serializer/deserializer
SIM	subscriber identity module
SiP	system-in-package
SMA	sub-miniature version A
SMT	surface mount technology
SOA	safe operating area
SoC	system-on-chip
SoP	system-on-package
SP	standard practice
SPD	surge protected device
SPICE	simulation program with integrated circuit emphasis
TCAD	technology computer-aided design
TIVA	thermally induced voltage alteration
TLP	transmission line pulse
TLU	transient latch-up
TSV	through silicon via
TV	television
TVS	transient voltage suppression
TX	transmitter
USB	universal serial bus
UV	ultra violet
VDD	positive voltage supply
VFTLP	very fast transmission line pulse

3 Terms and Definitions (cont'd)

VHDL	Verilog hardware description language
VSS	negative voltage supply
WP	white paper
WSP	wafer scale package
XTAL	crystal oscillator

Crosstalk: Any phenomenon by which a signal transmitted on one circuit or channel of a transmission system creates an undesired effect in another circuit or channel. This phenomenon is usually caused by undesired capacitive, inductive, or conductive coupling from one circuit, part of a circuit, or channel, to another.

EMC: electromagnetic compatibility – The condition which prevails when telecommunications (communication-electronic) equipment is collectively performing its individual designed functions in a common electromagnetic environment without causing or suffering unacceptable degradation due to electromagnetic interference to or from other equipment/systems in the same environment (MIL-STD-463A).

EMI: electromagnetic interference - 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.

External Pin (interface pin): An external pin is one which at the board/card level is exposed to potential ESD threats from the outside world.

FR-4 (or FR4): A grade designation assigned to glass-reinforced epoxy laminate sheets, tubes, rods and printed circuit boards.

Hard Failure: Failure of a system due to physical damage to a system component which can only be repaired by the physical repair or replacement of the damaged component.

IEC-Robustness: The capability of a product to withstand the required IEC ESD-specification tests and still be fully functional.

IEC ESD event: An ESD stress as defined in IEC 61000-4-2.

Immunity: The ability of an electronic device to function properly in its electromagnetic environment.

Internal Pin (non-interface pin): An internal pin is one which is exposed to ESD threats typically only during IC manufacturing or during a crosstalk situation at the system level.

Residual Pulse: The resulting voltage/current (after system level ESD protection devices) seen by an IC component from an IEC stress waveform.

Second breakdown trigger current - I_{t2} : The current point at which a transistor enters its second breakdown region under ESD pulse conditions and is irreversibly damaged.

3 Terms and Definitions (cont'd)

SEED: System-Efficient ESD Design - Co-design methodology of on-board and on-chip ESD protection to achieve system level ESD robustness.

Susceptibility, conducted: A measure of the interference signal current or voltage required on power, control and signal leads to cause an undesirable response or degradation of performance (MIL-STD-463A).

Susceptibility, electromagnetic: The degree to which an equipment, subsystem or system evidences undesired responses caused by electromagnetic radiation to which it is exposed (MIL-STD-463A).

Susceptibility, radiated: A measure of the radiated interference field required to cause equipment degradation (MIL-STD-463A).

Susceptibility threshold: The signal level at which the test sample exhibits a minimum discernible undesirable response (MIL-STD-463A).

System level ESD Robustness: The capability of a product to withstand the required IEC ESD-specification tests and still be fully functional.

Soft Failure: Failure of a system, not due to physical damage, in which the system can be returned to a functional state without the repair or replacement of a component. Return to a functional state may or may not require operator intervention. Operator intervention may include rebooting or power cycling. Soft Failures can involve software issues and software fixes but in the context of this document they are primarily due to ESD events injecting unwanted signals into the system which place the system into a state in which it does not function as intended.

VHDL-AMS: Verilog-AMS is a derivative of the Verilog hardware description language. It includes analog and mixed-signal extensions (AMS) in order to define the behavior of analog and mixed-signal systems. It extends the event-based simulator loops of Verilog / System Verilog / VHDL, by a continuous-time simulator, which solves the differential equations in analog-domain. Both domains are coupled: analog events can trigger digital actions and vice versa.

4 Background and Outline

4.1 History of the Industry Council on ESD Target Levels

The Industry Council on ESD Target Levels (Council) was formed in 2006 to address a growing disconnect between original equipment manufacturers (OEMs) and manufacturers of integrated circuits (ICs) with regard to electrostatic discharge (ESD). The competitive environment requires that OEMs create products with higher performance in ever smaller form factors while maintaining and improving reliability and offering the products at competitive prices. This progress was made possible by imposing the following improvements in ICs; higher levels of functionality, higher speeds, smaller component size and lower power. That is, the burden of higher performance has been transferred to the IC suppliers, who must achieve these improvements through enhancements in their chip designs. IC manufacturers have been able to make these improvements by employing new IC technologies with smaller feature sizes to improve functionality and speed and lower working voltages to prevent wear-out of the circuit and maintain reasonable power levels.

OEMs of course need these improvements, but they do not want them at the cost of reliability and yield. OEMs therefore maintained the same quality and reliability requirements on ICs produced in the latest technology as they had for a more mature product. One of these requirements was for the ESD robustness of ICs. 2 kV of human body model (HBM) robustness had long been a *de facto* standard and 500 V of charged device model (CDM) robustness was becoming a similar requirement. Also, there was an unintended, albeit perceived important, requirement that the ICs must simultaneously meet 200 V for the machine model (MM). However, starting around the 90 nm technology node, IC manufacturers were finding it increasingly difficult, and sometimes impossible, to consistently meet these requirements. The smaller feature sizes, lower operating voltages and high speed signal requirements of ICs were shrinking the design window available for ESD protection. IC manufacturers, however, knew that 2 kV HBM and 500 V CDM levels were not needed. HBM and CDM tests are performed to ensure that ICs can survive manufacture in an ESD controlled manufacturing facility. Experience has shown that with basic ESD control procedures, ICs with far lower HBM and CDM levels could be handled. Furthermore, without basic ESD controls, robustness far beyond 2 kV HBM and 500 V CDM will not survive. Attempting to meet 2 kV HBM and 500 V CDM was therefore costing the industry millions of dollars in redesigns and delays to market without any benefit to the industry.

The Council was formed to show the electronics industry that lowering ESD levels from 2000 V HBM and 500 V CDM was not only possible without sacrificing quality and reliability, but also the right thing to do. “JEP155: A Case for Lowering Component Level HBM/MM ESD Specifications and Requirements” [1] demonstrated why it was becoming more difficult to design high levels of HBM performance in advanced technologies and presented data that proved lower HBM levels do not lead to higher levels of failure. JEP155 also showed that designing for HBM would guarantee adequate levels of intrinsic MM performance and that specifically testing for MM was not necessary. “JEP157: A Case for Lowering Component Level CDM ESD Specifications and Requirements” [2] made a similar case for CDM levels below 500 V by presenting explanations of why high levels of CDM performance were not necessary and presented data to back up the arguments.

4.1 History of the Industry Council on ESD Target Levels (cont'd)

JEP155 (WP1) and JEP157 (WP2) were influential in changing the industry's mind about the level of ESD robustness needed to allow high yield manufacturing of systems. OEM's had a lingering concern however; what will lower component ESD levels do to system reliability? It has been assumed by many that the first step in producing ESD robust systems is to choose components with high HBM and CDM levels. The assumption that higher HBM and CDM levels will automatically produce ESD robust systems seems logical, but members of the Council knew this assumption was not true and that it was blocking the adoption of more reasonable HBM and CDM levels. The Council decided to address the problem with a third white paper to demonstrate the lack of correlation between component level ESD and system level ESD, and to address the wider question of how to effectively design for system level ESD robustness. Although *ad hoc* system level ESD designs have been done in practice, the important message of the JEP161 (WP3 Part I) was to remove the misconceptions about system level ESD.

System level ESD is a very broad subject and differs substantially from HBM and CDM ESD. HBM and CDM tests only look for physical damage to unpowered ICs. System level ESD is most often performed on a powered and functioning system, and failures include not only physical failures but system upset. Due to the broad subject of system level ESD, WP3 has been divided into two parts. JEP161 focused on physical failures and the lack of correlation between component level ESD (HBM and CDM) and system level ESD. JEP161 also introduced the (basic) system-efficient ESD design (SEED) strategy for designing ESD robust systems. In this document, JEP162, we address the broader topics of system level ESD design and system upset by an advanced SEED concept. For those not familiar with JEP161 a summary has been placed in [Annex D](#). The remainder of this clause will preview the content of JEP162.

We would also like to reference a recently published white paper by JEITA which addresses system level ESD related tests of ICs as used by the Japanese Industry [3]. Tests based on 200 pF/0 Ohm and 200 pF/100 Ohm RC discharge circuits are discussed to characterize transient latch-up robustness of powered ICs. The JEITA white paper focuses on this specific test procedure while this white paper discusses the general design approach.

4.2 JEP162 (White Paper 3 Part II): Summary of Clauses/Annexes

[Clause 5](#) looks at how ESD affects systems, beginning with how these events are coupled to internal system circuits and devices, followed by the system response (both hard and soft failures) and concluding with analysis methods used to determine root causes of upsets and failures. Included are methods of categorizing failures and coupling modes to internal circuits. Also described are classic trouble-shooting methods for solving ESD upset problems plus new technologies capable of identifying sensitive circuit areas and components.

[Clause 6](#) examines the advantages and limitations of ESD/EMI design methodologies as they are presently practiced. State-of-the-art ESD/EMI design methodologies span the continuum from comprehensive theoretical 3D modeling of Maxwell's equations for an entire system to the most basic trial and error bench tests, and numerous advanced practical and theoretical tricks-of-the-trade in between. Utilizing one or more of these methods in the concept, design, and prototype phases, a designer can observe and improve the extent and effectiveness of any element or flow in a process intended to balance ESD/EMI robustness, system performance, and cost.

4.2 JEP162 (White Paper 3 Part II): Summary of Clauses/Annexes (cont'd)

[Clause 7](#) summarizes the SEED approach. In the SEED approach the path of the ESD stress is analyzed and predictions of system response are made using the properties of the printed circuit board and components on the board. Not all ESD paths are the same, however. ESD stress can range from high energy stresses, which are directly coupled from a system input/output (IO) connector to a sensitive pin on an integrated circuit causing physical damage, to a much lower energy stress that is capacitively coupled to sensitive circuit nodes and results in system upset, but no physical damage. This clause categorizes the types of ESD stress which a circuit can be exposed to and shows how different approaches and circuit properties will be needed to analyze the different stresses and prevent system failures.

[Clause 8](#) describes the models and analytical tools needed to support the SEED concept. The first requirement is a standard model for the description of integrated circuit IOs. After describing the requirements for a standard model, existing models are examined that may be extended or adapted for SEED requirements. Next, simulation tools that use these models are also examined for their adaption to SEED. This is followed by an examination of the limitations of both software and hardware analytic tools. Finally, an example using available models and tools is presented.

[Clause 9](#) presents a summary of the white paper and final conclusions. The white paper shows that there are tools available, such as transmission line pulse (TLP), which can study component properties in the ESD time and current domain as well as scanning tools which can measure the propagation of ESD events through a system and locate sensitive circuit nodes. The white paper categorizes the paths through which ESD stress can enter a system and outlines how to analyze and design for these types of stress. To use this increased understanding, design tools need to be upgraded to handle the information from the extended characterization tools and to perform the analysis needed to quantify the behavior of the paths through which ESD stress enters a system. The models used to describe components need to be modified to extend their useful range into the current, voltage and time domain of ESD events. Finally, component manufacturers need to characterize their products outside the range of normal operation so that system level ESD design can be done based on known component properties. This can only be done with extensive dialog between system designers, measurement equipment manufacturers, electronic design automation (EDA) tool vendors, model file developers and component suppliers. However, this paper does define the important issues and provides a starting point and significant first steps in this dialog.

[Annex A](#) addresses the typical stress conditions and design solutions used in various fields of electronic industry ranging from mobile phones, medical devices, computers, consumer electronics, and automotive components to avionics. It provides an overview of test standards to be applicable beyond IEC 61000-4-2 and discusses the impact of the multiple stress requirements on the design solutions. The applicability of the previously introduced SEED concept is analyzed for the various types of systems.

4.2 JEP162 (White Paper 3 Part II): Summary of Clauses/Annexes (cont'd)

[Annex B](#) addresses the changing technologies from different points of view that are slated to have an impact on the design capability of system level ESD protection. The main objective of the annex is to review the integrated circuit technology roadmaps and trends with consideration to the system level ESD performance of information technology (IT), communications, and automotive electronics. The various issues that are critical for these trends include IC package development into more complex 3-D structures, new advances in board assembly techniques, emerging optical interconnects as applied to IC connections, and the promising development of novel suppressive materials such as polymers with embedded nanoparticles that can potentially offer low-capacitive and efficient solutions at both the package level and the board level. In its overall essence the annex assesses the impact of rapidly advancing technologies on system level ESD requirements and designs. While not specifically recommending any future system level ESD specs, the annex points to where the difficulties could arise from scaled down technologies, higher speed circuit designs, and broader analog and high voltage applications. The annex also attempts to include some comments on the demands for resources and the cost for system ESD designs from the perspectives of both IC suppliers and system builders.

[Annex C](#) describes how ESD threats to systems include both a fast component, from the ESD gun's initial current spike, followed by a slow component, with lower current but with considerably longer duration. The Annex explains how the current paths for the two components can be very different, can cause different types of failures and require different solutions. The section ends with diagnostic suggestions for locating susceptible areas within a system or circuit board.

5 Overview of ESD Stressing and System Response

The purpose of this clause is to look at ESD system level testing as it is done today as well as the complications (including coupling issues), failure modes, and trouble-shooting methods used to determine root cause of failures. “Soft” failures, where no obvious component damage occurs, and “hard” failures, where component damage *is* apparent, are discussed in some detail. Considerable attention is placed on electromagnetic coupling modes and the propagation of electrostatic discharges in a system. New evolving methods such as susceptibility scanning, software tools and system specific test boards to monitor the health of a system are all discussed.

5.1 Presently Used Stress Tests for ESD

There are presently only a few basic stress tests used in the industry for testing systems for the effects of electrostatic discharges. These are:

- **IEC 61000-4-2** and its derivatives for compliance testing of virtually all consumers, telecommunications, medical and light industrial electronics.
- **ISO 10605** for automotive electronics.
- **DO-160** for commercial avionics.
- **CDE (cable discharge event)**. There are various corporate standards in use, and at this writing, Electrostatic Discharge Association (ESDA) is close to issuing a draft standard practice to help standardize test methods for CDE.

The following sections summarize these tests. For a more detailed discussion see JEP161, clause 5 [4].

5.1.1 IEC 61000-4-2

IEC 61000-4-2 applies a standard test methodology to equipment, systems, subsystems and peripherals that could be exposed to ESD events in the final installation. The environmental conditions (humidity, flooring materials, low-conductivity carpets, grounding methods) may influence the intensity of the discharge, which in turn affects the susceptibility to damage of the systems to an ESD event, and for the purposes of compliance testing, this standard closely defines the conditions under which testing is to be done. IEC 61000-4-2 specifies a current pulse that is quite different than those used for testing integrated circuits for ESD during assembly and packaging and is not correlative.

5.1.2 ISO 10605

ISO Standard 10605 is used to characterize the ESD sensitivity of electronic subsystems in road vehicles. This standard draws on the IEC 61000-4-2 for most of its procedures and physical set-ups, but adds three additional current impulse variants for conditions specific to the automotive environment. It applies to discharges in the following cases:

- ESD in assembly
- ESD caused by service staff
- ESD caused by occupants

ISO 10605 applies to all types of road vehicles regardless of the propulsion system (such as spark-ignition engine, diesel engine, electric motor) and for some cases requires testing to 25 kV.

5.1 Presently Used Stress Tests for ESD (cont'd)

5.1.3 DO-160 Section 25

This document is used to test airborne equipment (avionics) for the effects of static discharges from human contact. It is based on IEC 61000-4-2 and uses the same ESD test pulse. It consists of a 15 kV air discharge test applied to points on operating avionics that are accessible to people.

5.1.4 CDE Testing

This test is designed to determine the susceptibility of electronic products to electrostatic discharges that occur when a cable, such as Ethernet or universal serial bus (USB), are connected. If a charge differential exists between the cable and the product being connected, a discharge will occur to the affected IO pins. A proposed ESDA document provides test methods using both the ESD gun and a modified TLP system.

5.2 Definitions

5.2.1 Hard vs. Soft Failures in Systems

Both hard and soft failures in an electronic system can be induced by transient events from outside the system, such as noise transients on connecting cables and electrostatic discharges, but also by over-voltages due to mis-operation or improper connection of the system. In any case, the system has ceased to operate as intended.

A “hard” failure is one where the outside event has caused damage to a component that will require a service technician to replace the affected component. Examples of hard failures include damage to gate oxide, resistors and metallization in the signal path which could have been as a result of latch-up or overvoltage. These will all be discussed in more detail later in this clause.

A “soft” failure is one where the outside event can have several effects. Using some definitions paraphrased from IEC documents, one can demonstrate these situations:

- System automatically recovers with no loss of data and no operator intervention. This upset is completely transparent to the operator. An example might be a change to a command or data stream that is caught and corrected by system software.
- System malfunctions in a way that the operator notices but operation continues. Examples might be interference to or momentary loss or distortion of a display, keystrokes that are temporarily corrupted or not recognized, or static or noise in an audio system.
- System malfunctions in a way that requires some recovery action be taken by the operator. Examples might be system lock-up, display becomes blank, controls or keyboard ceases to function. Typically, this kind of upset or malfunction requires powering down the system and re-booting.

In the above scenarios data could be corrupted or lost without being apparent to the operator. Under IEC definitions, loss of data is never allowed when testing a product.

5.2 Definitions (cont'd)

5.2.2 Sub-Assemblies and Modules

The definition of a system is generally considered to be a completed, self-contained product such as a cell phone or lap top computer; however, for testing purposes, a system can also be a sub-assembly or module such as a video card, engine control module (in the automotive industry), or other device which can only function as part of a larger self-contained or distributed system. Sub-assemblies such as these (except automotive) are now included under the European Union's EMC Directive and must be tested as systems with similar failure criteria.

Testing and evaluation of sub-assemblies and modules present an obvious problem: the device being tested needs to be operating in a larger system to properly test for susceptibility. Ideally, it should be tested in the actual system where it will reside, but this isn't always possible. Take for example the manufacturers of sound cards, video cards, memory modules and other devices that could be assembled into a wide range of systems. These manufacturers may elect to test their product in a typical installation – a computer with known susceptibility characteristics – or in a test jig. It's up to the manufacturer to decide the best way to test the product to insure compliance, and often a system manufacturer, who is going to purchase and use the sub-assembly in question, may require testing in a specific way.

5.3 Coupling of ESD into Systems and Circuits

5.3.1 How Does ESD Couple into a System and Affect a Specific Component During System Level Testing?

Depending on the requirements of the test standard, system level tests typically require discharges to system enclosures and controls and may include some externally exposed pins. IEC simulators produce currents and transient fields and the resulting current pulses have been described as having both CDM and HBM like characteristics. Furthermore, they induce strong electromagnetic fields, which are not necessarily associated with the discharge current; including those fields that are also excited by the discharge relay used for contact mode testing (i.e., the ESD current is directly injected into the test object through metallic contact between the tester and the device under test (DUT), as opposed to an air discharge between the tester and DUT). Annex D of the IEC 61000-4-2 standard (2009) [5] provides good insight and further details the effect of different sensitivities and coupling mechanisms [6].

During discharges to system enclosures the injected current pulse spreads at close to the speed of light over the metallic surface of a metallic enclosure. This occurs because the current must satisfy the tangential electric field boundary condition; $E_{tan} = 0$. This can only be fulfilled by the creation of a current on the surface. At locations on the enclosure where the current has to divert due to the presence of slots or openings, fields will couple from the outside to the inside of the enclosure causing transient electromagnetic fields inside the enclosure ranging from very small to very large (kV/m). Furthermore, the current pulses will reflect on edges of the enclosure and couple to attached cables, predominately in common mode, which can then be converted to differential mode currents and possibly cause system upset.

5.3.1 How Does ESD Couple into a System and Affect a Specific Component During System Level Testing? (cont'd)

The current densities flowing on the inside of the enclosure, its cables and PCBs are associated with strong electromagnetic fields. The electric fields can couple capacitively while the magnetic fields will induce voltages in any loop they can penetrate. The net effect of the dynamically changing electric/magnetic field strengths and localized field are induced voltages and currents. The induced voltages are often pulses of < 2 ns in width. Typical coupling scenarios are:

- A current flowing on the outside of a personal computer (PC) close to the peripheral component interconnect (PCI) slots of the enclosure will couple from the outside to the inside as the PCI slots are not well connected. Once the fields enter the inside, they can couple to any board, such as a graphics card, upsetting that board.
- The current from one PCB is coupled to another PCB connected by a flex circuit cable. The flex circuit cable does not confine the fields of the wanted signals well, and as a consequence the common mode current of the ESD on the flex cable can couple easily to signal traces.
- A current is injected into an audio trace, which is robust against ESD. This trace is routed inside the PCB parallel to a reset line. The coupling between the audio trace and the reset line causes noise pulses on the reset line; upsetting the system.
- A charged cable is plugged into a USB port. The ground contacts first and a large current is injected into the shell of the USB connector. This will cause a voltage drop between the USB connector shell and the chassis (as the connection is not perfect, but it forms a small inductance). The voltage between the shell and the chassis is visible on both the outside and the inside of the enclosure, and will force a current on the inside of the enclosure. Furthermore, although the shell connected first, a voltage is induced on the differential pair, which may upset a USB hub.

The fields can also interact with the direct current (DC) voltage supplies. While this is likely to lead to upsets if an IC's internal power nets receive large amounts of current from an ESD event, it is unlikely to upset power planes on circuit boards. The high decoupling capacitance and low impedance of typical board supply planes tend to limit the induced voltage, consequently, upset or damage is seldom seen by ESD injection to circuit board power planes. If power plane or ground plane injection causes ESD upsets, the mechanism is not the result of DC voltage fluctuations, but rather due to the transient fields of the ESD event coupling into other nets or directly into ICs.

For test standards requiring discharges directed at exposed pins (such as USB ports) or plugged in fixtures that simulate system events like cable discharge, the current pulse will travel from the connector to board traces which direct charge to the component pin. ESD injected into an input or output pin will typically be diverted to the internal positive voltage supply (VDD) and negative voltage supply (VSS) net within the IC. However, the internal voltage transient can cause soft failures or hard damage. The effect of both signal and supply transients will be discussed in more depth later in the clause.

Depending on board layout, trace length/thickness, signal shielding, and the passive/active components connected to a board trace or plane, the resultant reactance of the signal trace will attenuate rise time, duration and peak current as seen by the targeted IO or supply pins. This ultimately affects what happens to the charge when it gets into a system.

5.3.2 What Happens When the Charge Gets into the System?

The hybrid CDM and HBM characteristics of IEC simulator pulses results in high peak currents and pulse durations on the order of 60 ns at the point of charge injection. The degree of ESD pulse attenuation/degradation before arriving at the part will determine how the on die IO and power supply protection reacts. Attenuation of a pulse that would otherwise exceed the built-in protection capability could help protect a part from damage. However, if the perceived pulse characteristics fall outside of the component protection design window, the attenuation could also inhibit the response of pin level protection circuits as well as the resistor/capacitor (RC) triggered supply clamp. The net effect of inhibited ESD protection response could be failure at voltage levels lower than those seen by a component during component testing.

Signal attenuation can affect the way internal supply rail power clamps engage to dissipate the charge that is dumped onto the rail when the ESD diodes turn on. Power clamps often use triggers that expect a certain voltage rise time to engage. If clamps engage quickly and their current shunting capacity is not exceeded, the device should be protected. If the clamps turn on too slow or not at all, overvoltage damage of transistors connected to the supply rail can occur.

Because component protection is designed for an unpowered component, the response of a component when power is applied in a system and IO pins are transitioning can be much different. In some cases, the response can be inhibited because the ESD protection circuits see voltage on output pins and DC bias on internal supplies. These voltages affect the threshold at which protection schemes, like double diode [2], turn on and consequently the ability of the pin level protection circuits to shunt current. ESD power clamps that expect to see ESD pulses with the part unpowered now see pulses on top of a pre-existing DC bias. This voltage starting point, along with the possibility of a change in the time constant of an ESD pulse due to a reactance contribution from the voltage regulator, can retard the response of the power clamps.

The scenarios described above do not take into account external signal/power protection that may reside on the board to protect from system events. Transient voltage suppression (TVS) components protect a component by shunting charge before reaching the component. However if the TVS component does not fully shunt the signal, and the rise time of the residual IEC gun pulse is not fast enough to engage the on die supply clamps, overvoltage damage can occur as described above.

Coupling to signal or power lines adjacent to a targeted signal line can also lead to failure in signals or supplies that are not stressed directly. These lines may not have the same degree of protection as lines leading to the outside world. Failure of these lines will depend on the degree of coupling and protection on the coupled IO or supply.

5.3.3 Recoverable or “Soft” System Failure Modes

Many of the IO and power supply overvoltage/transient issues that cause hard failures at a given voltage may cause recoverable or soft failures at a much lower voltage, causing a system upset or a change of state in the system. Typically, the upset levels are much lower than the destruction levels. Signal or voltage supply rail (such as VDD or VSS) pulse induced transients is one mechanism that could lead to a loss of state of a system component, requiring user intervention to reset the system. Transient latch-up due to ESD pulse induced power glitches, or locally induced overvoltage of a power domain or cluster of transistors in a discharge path is another mechanism that could lead to a loss of state of a component/system.

5.3.4 System Degradation

In theory, so called “soft damage” to a transistor could lead to system performance degradation, which could be considered a system level failure if the degradation is self-detected by the system. An example would be soft oxide damage to an output driver transistor of a stressed pin which affected the robustness of the transistor. The driver could continue to operate satisfactorily at low frequencies, but higher frequencies or low supply voltage could lead to failure. Soft oxide damage due to voltage transients on voltage supply rails could also lead to degradation of internal circuit paths that ultimately affect performance as well. Passive components on system boards can also be damaged to the point that performance is degraded. Examples are surface mount chip capacitors and resistors used for filtering or terminations. Over voltage/current damage can change the effective value of these components to the point the circuits malfunction if they continue to degrade after initially being electrically damaged. This is sometimes referred to as a “latent” failure: one which occurs at a later time due to damage from a transient at an earlier time.

5.3.5 Hard System Level Failure Modes

Unlike a functional powered up system which can put a component in many states (and consequently induce many different types of failures), the state of a standalone component prior to the initiation of component testing is constant. System level testing can induce hard failures that would appear similar to those seen in component testing. There are extra failure modes that can occur in system testing that don't occur in component testing, but some of the more common component testing failure symptoms that could be seen in system level testing includes [7]:

- a) Damage to gate oxide and/or channel damage to drivers and receivers attached to an IO signal.
- b) Damage to primary signal path ESD protection circuits such as ESD diodes whose purpose is to protect the signal path. This occurs when the robustness of the protection circuit is exceeded.
- c) Damage to resistors and metallization in the primary signal path.
- d) Overvoltage damage to transistors which reside in power domain(s) and absorb charge routed to them by the ESD protection circuits. This occurs when the protection circuits (diodes, clamps, etc.) for the power domain fail to respond fast enough or their robustness is exceeded.
- e) Latch-up

Because component protection is designed for an unpowered component, the response of a component when power is applied and IO pins are changing state is much different. In some cases, the response can be inhibited. This can be due to the following causes:

- a) ESD protection circuits on IOs, such as protection diodes between the pin and internal VDD rails, are designed to shunt to unpowered rails. Voltage on the rail affects the effective voltage threshold of the protection diodes. For a diode with the anode connected to the pin and the cathode to VDD, the voltage threshold increases with bias. Elevated thresholds result in higher pin voltages during discharge, which typically increases the voltage seen by downstream circuits during a discharge.
- b) dV/dt (for example, RC) triggered ESD overvoltage internal supply clamps that expect to see ESD pulses with the part in an unpowered condition now see pulses that start from a powered condition. This pre-existing voltage, along with the possibility of a change in the RC trigger time constant due to a reactance contribution from the voltage regulator, can retard the response of a clamp trigger circuit.

Aside from traditional component level ESD damage and damage due to inhibited ESD protection, localized voltage differentials which are not seen in standard operation could lead to latch-up of transistors. This can cause hard damage to a component if the latch-up condition is sustained. In theory, signal corruption due to an injected pulse could lead to a loss of state and signal “contention”, where transistors are simultaneously driving opposing signals that lead to electrical overstress and permanent damage if sustained.

5.4 Troubleshooting to Determine the Cause of Failures

5.4.1 Hard Failures

Classic methods of troubleshooting electronic products work well in the case of hard failures. Faulty sub-systems, boards and finally components are systematically isolated by measurements of power supplies and signal tracing. In the case of hard failure of a component, damage is often detected with methods such as photon emission microscopy (such as emission microscopy (EMMI)) and/or laser induced circuit perturbation (such as thermally induced voltage alteration (TIVA)) that highlight circuit damage. These are well understood and documented techniques [8], and as such, won't be dealt with in this paper.

5.4.2 Soft Failures

Classic troubleshooting methods don't work well on soft failures simply because there is no physical evidence to find. Either the system recovered on its own through error correction routines or re-booting the system corrected the error. Soft failures are often found during compliance testing for ESD (as well during other types of immunity testing) but they also occur in field at the customers' site. In either case, the root cause of the failure needs to be determined and corrections made to the system to prevent further upsets.

When a soft failure is detected, the method of troubleshooting is often trial-and-error. This can be effective when the person doing the troubleshooting is familiar with the system, but if the failure occurs in the field or at an outside compliance lab that may not be the case. Even for a soft failure being investigated by someone familiar with the system architecture, the real root cause may still not be resolved although the symptom may be eliminated. Filtering, shielding or the addition of protective components can be effective at removing the symptom, but the root cause might actually be a power bus running too close to a sensitive control line. Adding components may resolve the soft failure issue, but the real root cause -- the design problem -- remains un-detected.

One method of localizing a soft failure problem that is sometimes used is injection of a localized magnetic field or other disturbance in the vicinity of the suspect circuit. By moving the probe around the circuit and watching for upset it may be possible to determine the area of a board likely to be the problem. This method has recently been automated to allow very precise scanning and provide a 3-dimensional picture of a circuit board's weak spots and will be described in detail in the following section.

5.5 New Technologies for Determining Root Cause of Failures

5.5.1 Susceptibility Scanning

As discussed above, once a system fails due to a system level ESD event, isolating the root cause can follow different paths. For soft failures the most promising tool is local magnetic or electric field injection using susceptibility scanning. This can be performed by hand as previously mentioned but it is very difficult to obtain significant precision or generate a visual picture of the boards' sensitive locations. When done automatically [9, 10], these difficulties are removed and the ability to generate data for later analysis is achieved [11].

The objective of susceptibility scanning is to identify locations, ICs, modules and electrical nets that exhibit the same failure symptoms that were observed during system level testing. If those locations are found within the system, it is likely that during system level testing energy is being coupled from the outside to those locations, thereby causing the failure.

5.5.1 Susceptibility Scanning (cont'd)

To identify these sensitive locations a locally strong field needs to be created that resembles the noise that might be coupled from the outside ESD generator to the suspect board or circuit. The methods are detailed in [9, 10]. In brief, a transmission line pulser having rise times of < 1 ns is connected to magnetic and/or electric field probes. These field probes are moved close to the ICs, nets or modules in question and pulses are applied by the TLP, which induces the field. The system reaction is observed. By varying the probe type, size and applied voltage, locally sensitive regions can be identified. Further, the results can be visualized as susceptibility sensitivity maps as shown in Figure 3 and Figure 4.

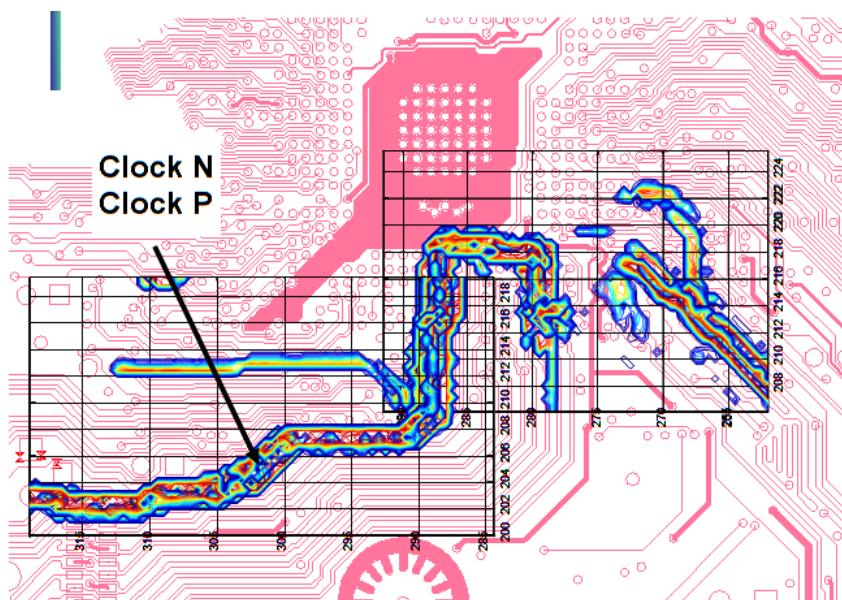


Figure 3 — Result of susceptibility scanning: Sensitive differential clock on a motherboard [9]
(Courtesy of Amber Precision Instruments)

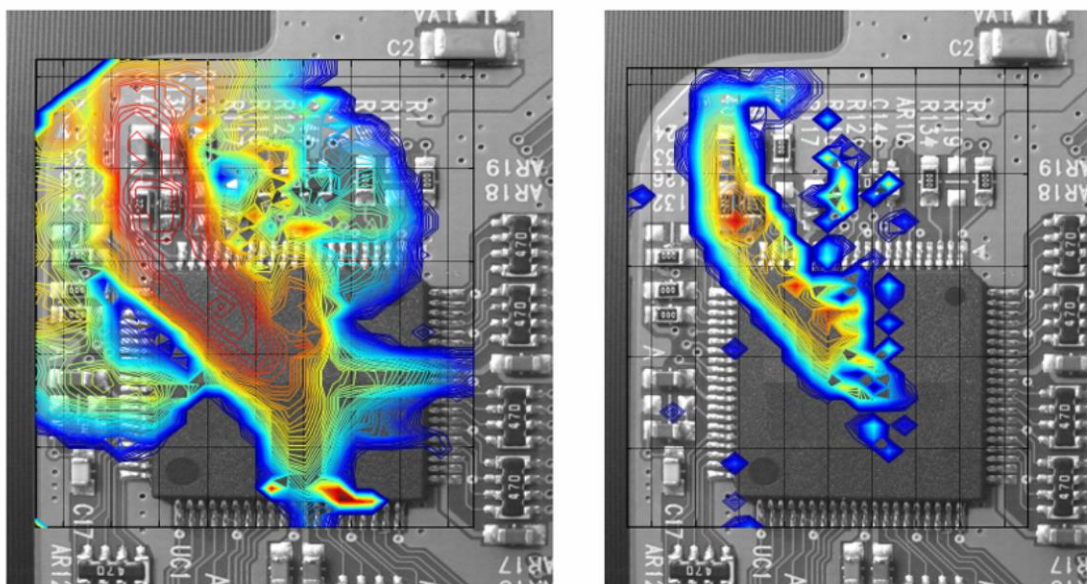


Figure 4 — Result of susceptibility scanning: Comparison of two functional identical ICs from different vendors. The color grade indicates the TLP charge upset voltage with blue being 4 kV, red being 1 kV [9] (Courtesy of Amber Precision Instruments)

5.5.2 New Software Methods

In addition to susceptibility scanning, software based methods can be used to uncover the root cause of ESD failures. These methods often require having pre-existing diagnostic tools built into the system that are targeted for debug. For system upset, where some system functionality is retained, software tools that collect the contents of die data registers can reveal status register bits, error codes, data loss or data corruption. All of this will provide insight into the nature of the failure. Other software tools include error handling routines that collect system response data for diagnosis but again, some system functionality must be retained to run the software diagnostic [12,13].

If system functionality is lost but components are accessible through special test modes such as JTAG (Joint Test Action Group) ports, it can provide another means of accessing the data registers. Factory debug and test modes can also be employed if they are available with appropriate documentation from the component manufacturer. Ultimately, for these tools to work, the system analyst needs to have a good working knowledge of the system and the information that can be extracted from the components.

5.5.3 System Specific Test Boards

System specific debug test boards are boards that can be embedded in a system to track and save system status for recall in the event of an ESD induced fault. Dedicated system monitor chips that report system status could also be used. Simple methods include fault indicator lights or display screen messages/codes that can point to unusual power consumption conditions by a component or else report the status of a component pin that only comes on during a specific fault condition.

When a failing component is identified and diagnostic information is gathered, component debug tools can be employed to isolate a particular location on a component. If the failing component can be exercised in the system to the point of demonstrating the mode of failure, various diagnostic tools can be employed including optical and infrared emission cameras and laser based scanning tools to pinpoint damage sites on silicon. Complications associated with use of these tools include special die preparation (die thinning) to support the optical nature of these tools. Software and/or system functionality may need to be modified to increase the acquisition rate of the optical signal. If the component cannot be operated in the system, it may be necessary to use special test hardware in conjunction with knowledge of the component to stimulate the failing condition. The complexity of the hardware can range from sophisticated automated test equipment (ATE) testers to curve tracers or DC power supplies.

Once a failure location is isolated, the next step is to understand the implications of the location of failure and, in some cases, the mechanisms seen in the physical analysis. Software based design tools that can correlate physical locations to circuit schematics are particularly useful for this analysis. The schematics can then be evaluated through analog circuit simulators such as simulation program with integrated circuit emphasis (SPICE) or digital simulators such as Verilog to confirm that the physical failure symptoms match both the analog response to ESD stimulus and the system behavioral response to the ESD upset.

As the response to a system failure becomes better understood, examination of physical die layout may be appropriate:

- If latch-up is suspected, the layout can be examined for latch-up design sensitivity.
- If damage to gate oxide is suspected, the circuit path that results in overvoltage during the stress event must be understood.
- If metal shorts or opens are discovered, the current carrying capacity of the metal routing at the affected location can be compared to the current expected during the system stress event.

5.6 Summary

It is important to recognize that both hard and soft failures occur as a result of ESD events in the test lab and in the field, and both need to be addressed. Component manufacturers rate components for their ability to withstand a certain voltage during handling, but an ESD event to a system producing only a few volts on an input pin of that component may cause a system to re-set unexpectedly. Fortunately, new software analysis methods and test instruments are becoming available to enable us to see what’s happening as the result of an ESD event. This enables both the component and system manufactures to make good decisions in design that will save money and benefit everyone.

6 State-of-the-Art ESD/EMI Co-design

Introduction

The threat to a design posed by ESD is essentially defined by the term “Electrostatic Discharge,” that is, the movement of an accumulated positive or negative static charge from the user environment to (or from) a component. The intensity of discharge that the component can withstand without damage or functional degradation defines its robustness and affects its cost.

Existing state-of-the-art ESD/EMI design methodologies span the continuum from advanced theoretical 3D modeling of Maxwell’s equations for a system to the most basic trial and error tests, and all of the limited practical and theoretical implementations in between. A matrix of these approaches is presented in Table 1.

Table 1 — Practical and theoretical co-design methodologies for ESD/EMI robustness

		Methodology Type	
		Practical	Theoretical
Complexity & Cost	Basic	Designer's experience, lessons learned, design reuse	Datasheet comparisons
	Advanced	Component qualification testing	SPICE modeling of ESD injection
	Comprehensive	Rigorous head-to-head system level iterative testing	Full 3D Maxwell Field-Solver Simulations

The overall design methodology is ultimately chosen to help the designer compromise on an optimum fixed point in the “tradeoff gamut” between three generally conflicting goals: (1) ESD/EMI robustness and susceptibility resistance, (2) signal integrity and functional performance (bandwidth, data-rate, minimum emissions, etc.), and (3) cost and/or time to market as depicted in Figure 5.

6 State-of-the-Art ESD/EMI Co-design (cont'd)

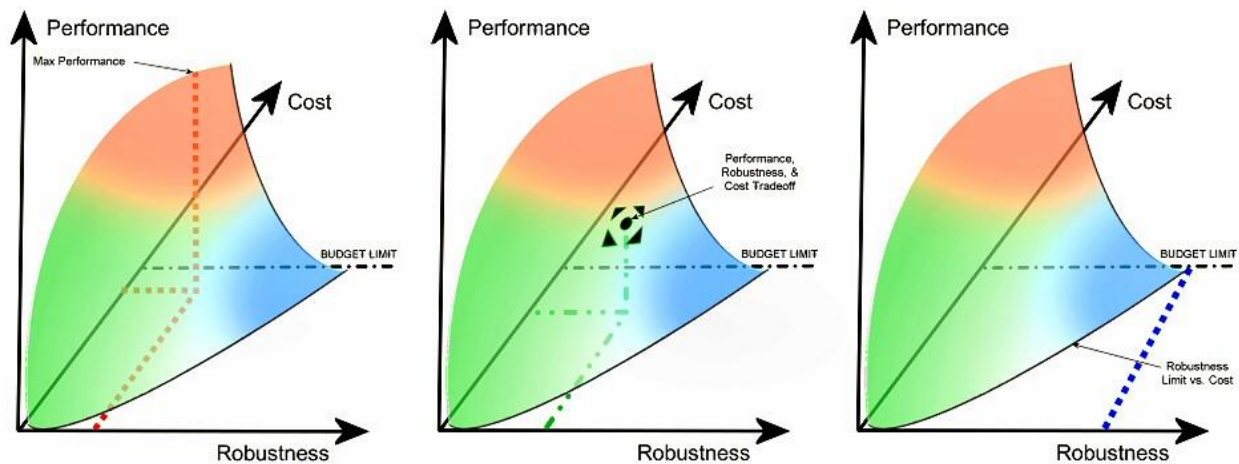


Figure 5 — ESD/EMI Co-Design Tradeoff Gamut

This concurrent shepherding of sometimes cooperative but often conflicting design goals during product design and development is referred to here as the “ESD/EMI Co-Design” problem.

Not surprisingly, many of the protection strategies for ESD are tightly related to EMC robustness and EMI suppression methods. This clause examines the advantages and limitations of existing and emerging methodologies in the art with respect to their effectiveness in arriving at the optimum robustness/performance/cost tradeoff for a given application. Obviously, the survey of such an extensive field is necessarily limited in its depth, but specific recommended system design guidelines are proposed.

From the beginning of the design process, critical exposed and susceptible nets must be identified and assigned reasonable and sufficient robustness levels, including the excess robustness protection margin desired. Aggressor pulse entry points or entry paths (whether conducted or induced) for hard and soft failures should be outlined as described in Clause 5. Component selection, layout and placement should be considered with regard to ambient and direct ESD/EMI strikes and disturbances and the effect on signal integrity. System partitioning, grounding, clamping, shielding and return path shaping are also considered, along with the problems of potentially hidden multiple/secondary discharge points within the system.

By managing these issues in the concept, prototype, and design phases, a designer can observe and improve the extent and effectiveness of any element or flow in a process intended to balance ESD/EMI robustness, performance, and cost with existing and emerging methodologies. The remainder of this clause will examine common examples of co-design as presently practiced, from the most basic rules of thumb, through advanced practical and theoretical methods, to comprehensive modeling of systems.

6.1 The Basics

As with any endeavor, a strong foundation or solid beginning can provide the most “Bang-for-the-Buck” in robustness vs. cost. Adherence to a few basic ESD/EMI principles and concepts throughout the functional design is often all that is needed to design an ESD robust system.

6.1.1 Shielding

The purpose of connecting a lightning rod and ground cable on a building is to route and shunt a potential lightning strike safely to ground in a reasonably controlled manner, away from flammable interior and structural components. Beyond encasing the building in a continuous Faraday Cage, the uncertainty and complexity of a strike makes the safe and cost-effective routing of the strike around delicate structures very difficult.

Consistent with ESD strikes on electronic systems, the primary goal for robustness design is to anticipate ESD entry points, and try to plan for effective return paths away from sensitive components.

While managing these primary effects, the designer also must be aware of potential indirect secondary effects of strikes or zaps, such as transient latch-up, or secondary discharges as described in Clause 7.

The first and generally most effective method of protection is to encapsulate the entire system in a conductive enclosure, but as system input and output ports often do not permit complete enclosure, it will be necessary to add some holes in the enclosure for buttons, displays and connectors. These holes then become potential entry points for system level ESD strikes.

When these entry points are identified on or near susceptible nets (whether directly injected or indirectly coupled as discussed in Clause 5), then discrete and/or on-chip protection circuits are often used in an attempt to catch and shunt ESD energy from the circuit back into the shield, and these methods are discussed in more detail below.

Good implementation choices made about how and where to implement limited shielding often provide the first and only protection needed for a sufficiently ESD-robust system. For example, certain systems naturally are constrained to certain standard IO connector requirements. A television (TV) or a monitor may require a high definition multimedia interface (HDMI) or digital visual interface (DVI) input. But whereas the bare HDMI connector presents tightly packed IO pins with interleaved ground pins and an enclosed ground shield as shown in Figure 6, the 0.100" (2.54 mm) pitch of the DVI pins exposes sensitive IO lines to potential unprotected strikes.

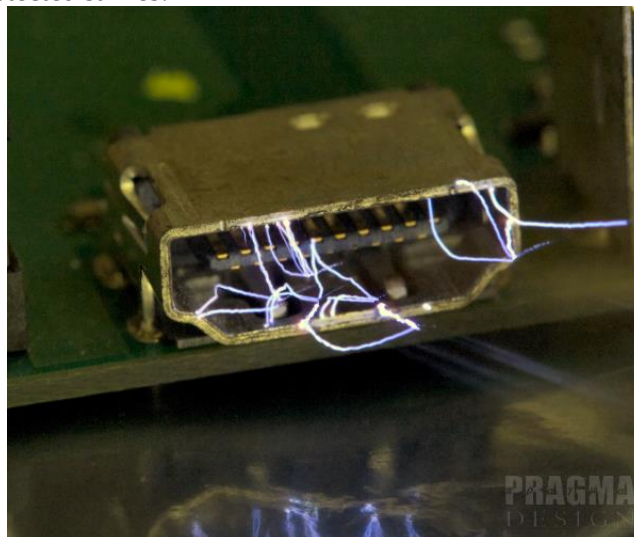


Figure 6 — Multiple air-gap strikes to shield and pins as an entry point or aperture

A system is as vulnerable as the first component to fail during an ESD strike. But the mere selection of an interface type may also introduce some engineered “ESD robustness” embedded in the basic design of the interface (such as the connector grounding design mentioned above). Thus basic knowledge of typical IO susceptibilities may provide a large portion of the solution.

6.1.2 Beyond Shielding

Signals into and out of a system must be designed to handle the potential of unwanted ESD entry through those points. Once such a potential is identified, the design engineer must provide a preferential path to dissipate the strike(s). The following are the basic points to consider from the ESD perspective:

- **Good Return:** Provide good ESD ground return paths for connector shells and grounds, and TVS or other ESD attenuation components.
- **Short Path:** Clamp and divert ESD charge as close to the entry point as possible. Place TVS components or other attenuators as close to the entry point as possible to limit the total loop area and direct coupling of the aggressor pulse into safe paths.
- **Hidden Impediments:** Minimize secondary parasitics in the return path (for connectors, grounds, and clamping components). Consider component package parasitics and PCB plating/stackup considerations which may affect overall system parasitics.

For a more detailed conceptual analysis of guiding ESD current from the entry point out of the system, see Annex C.

6.1.3 Component Selection

Any given system board will be populated with components of varying individual ESD robustness and protection. The same set of components implemented in different ways on the board, or within the system, may result in different levels of system ESD robustness.

While system specifications such as IEC 61000-4-2 are often applied to component evaluation boards as the “System-Under-Test,” the results of these tests cannot be directly compared to system level testing of complete, end-user ready systems. Component suppliers are limited in their ability to accurately characterize the system level robustness of their particular component since the choice of other interconnected components, connectors, routing and enclosures is out of their control and up to the system designer. Even if a component supplier provides a “reference design” circuit with a particularly well-characterized TVS component combination, a poorly designed enclosure can dramatically affect overall system robustness.

For example, consider an ESD stress to an IO pin of an integrated circuit. If the IO is intended to be connected directly to a system IO, such as a USB or HDMI pin, it would seem that stressing the component’s IO pin versus the component’s ground pin would correlate directly to the IO pin’s ESD performance in a system. The current path for a component ESD test may, however, be totally different from the current path during a system level ESD test. In a component ESD test, such as HBM, one pin combination (other pin combinations would look at IO to power rail or other IO) tests between the IO and ground, all current entering the IO pin must exit from the ground pin(s). In a system ESD test the current may all enter into the IO pin but the return path to the ESD source may include one or more power pins and have very little current exiting the integrated circuit through the ground pin(s).

6.1.3 Component Selection (cont'd)

Selection of components and optimal layout for the system may be the only degrees of freedom that a board or subsystem designer may reasonably have at his disposal. Determining component robustness from manufacturer specifications is not always straightforward. For example, consider the two TVS clamping components in Table 2:

Table 2 — Sample attempt at comparing and contrasting two TVS datasheets

	Component A	Component B
ESD “Rating”	10 kV ???	8 kV IEC 61000-4-2
R_{DYN}	0.8-1.2 Ohms *IEC 61000-4-5 (8/20us)	0.6-0.7 Ohms *TLP 100ns
V_{CLAMP}	18 V *IEC 61000-4-5	240 V peak ???
Strikes	10 kV - 10 positive / 10 negative 12 kV - 1 positive / 1 negative	8 kV - 1000 positive / 1000 negative

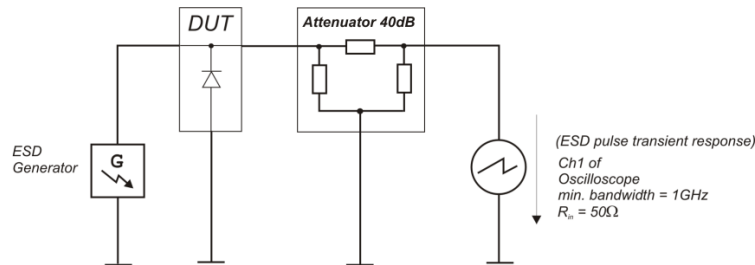
The 10 kV ESD withstand rating of the TVS protection component “A” on its evaluation board initially appears better than “B’s” 8 kV except that the test condition is not clear. But in any event, this only attempts to describe what the TVS component will withstand on its own, and tells nothing in particular about how well it can protect other components (For more information on the difficulties associated with testing components individually at the system level see JEP161, 5.2.2 [4], and Annex B.7 in this document).

The dynamic resistance is interesting in that it suggests that Component B might shunt more current from a node under protection than Component A, but upon further inspection we may find that the dynamic resistances are specified for different test conditions, test pulses, and stress levels. In the third row of Table 2, the “clamping voltage” is provided, although with a very low surge current (slow risetime, low bandwidth) in one, and a very high peak transient (fast risetime, high bandwidth) measurement setup in the other. In the end, the designer is left with essentially no meaningful comparison or contrast between the two sets of seemingly similar TVS parameters.

The last line of Table 2 reflects the attempts of some vendors to characterize the robustness with repeated strikes at a particular or multiple rated levels. These may imply a guarantee of survivability, in that either their component specifications will not change after repeated strikes, or that while the physical characteristics of the component may change dramatically within limits after repeated strikes, the absolute limits of the component specification will not be violated. While there is a maturing body of literature on repetitive damage in semiconductor and polymer clamp components, there presently is no accepted industry standard for the characterization or definition of “multi-strike” robustness or margin [14].

6.1.3 Component Selection (cont'd)

Even when components from the same vendor are considered under the same test conditions, the specification data may not provide meaningful comparative data for proper selection, especially when protection components are interacting with other components competing for ESD currents in a net and the sharing (and real-time behavior) becomes much more complex; see Figure 7a and Figure 7b for typical examples.



Symbol	Parameter	Conditions	Min	Typ	Max	Unit
$V_{CL(ch)trt(pos)}$	positive transient channel clamping voltage	$V_{ESD} = 8 \text{ kV}$ per IEC 61000-4-2; voltage 30 ns after trigger	[1]	-	8	V

Figure 7a — Example of a well specified ESD test condition, but with arbitrary test parameter reported

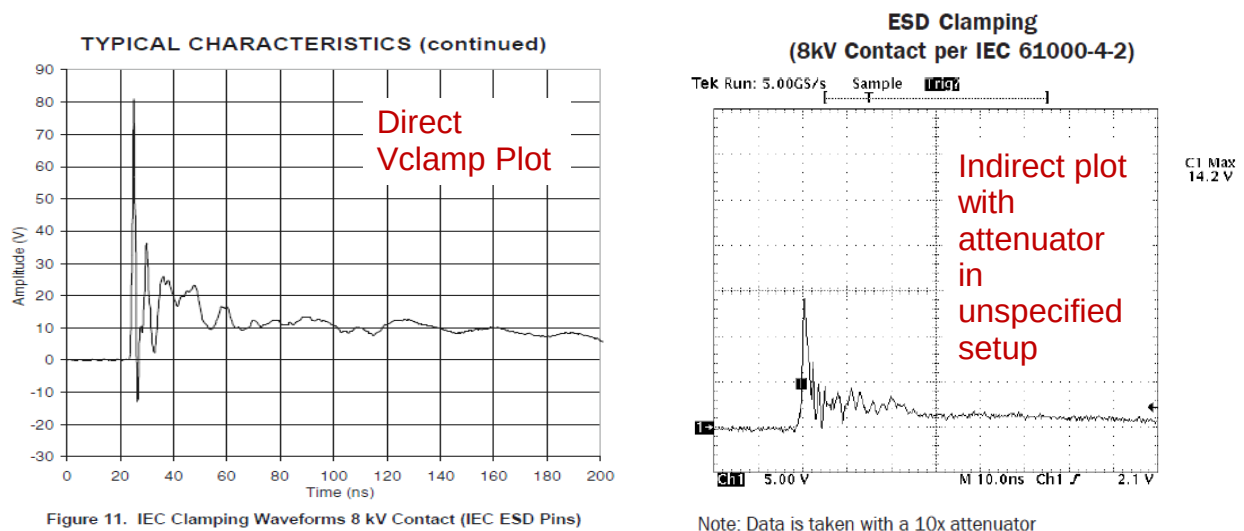


Figure 7b — Competing examples of unspecified ESD test conditions providing peak clamping values also affected by unreported measurement bandwidth and test conditions

The result is that design reuse becomes an important safety line for designers from one product generation to another in the realistic climate of incomplete ESD comparison data available to designers today. Lessons learned about replacing Component A with Component B may encourage the designer to stick with a known design, and render him less willing to consider a cost reduction of New-and-Improved Component C. Without a reliable methodology to qualify the performance in-house in specific systems, the designer may be forced to forgo an otherwise margin-improving cost reduction.

6.1.4 ESD/EMI Budget Strategy

For critical IO nets, such as high-speed serial interfaces or radio frequency (RF) antenna connections, the system designer may be faced with a passive parasitic budget as well as a bill of materials (BOM) pricing budget. As illustrated in Figure 8, similar challenges exist for EMI filter design and TVS clamp selection where there is a direct external interface with signal integrity restrictions on filter and protection components.

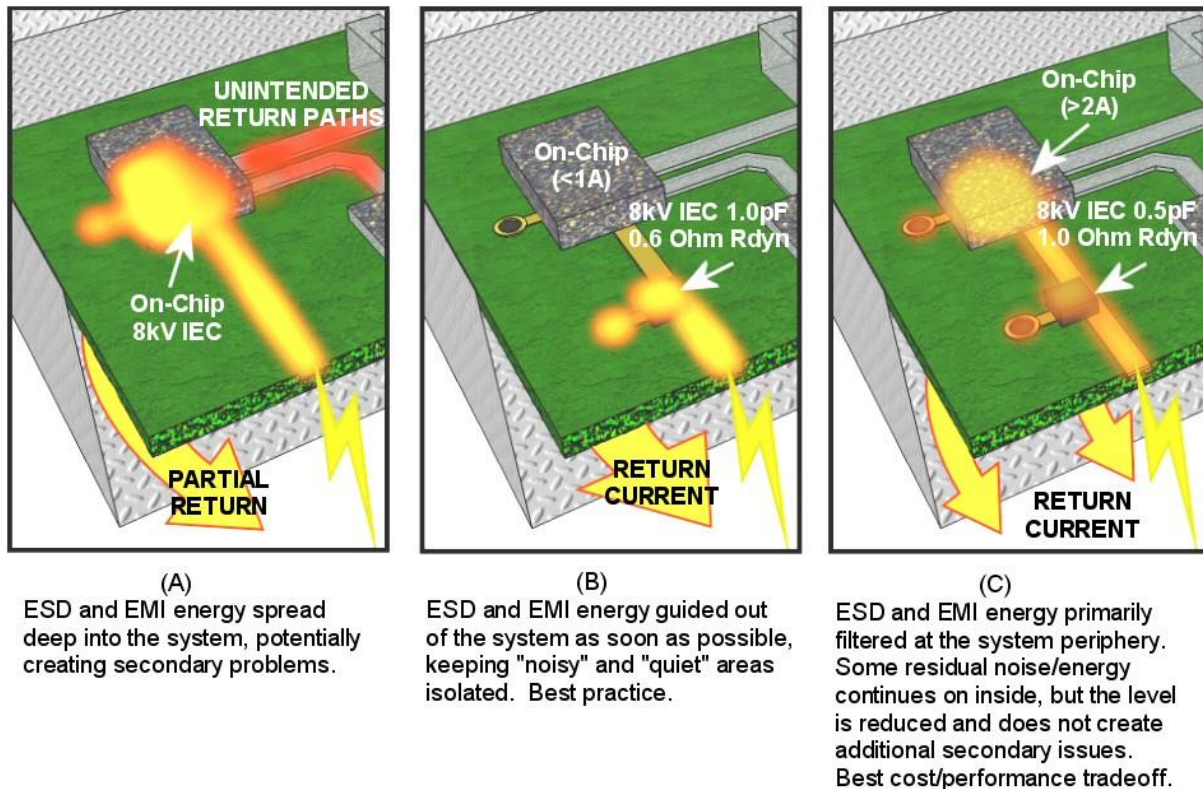


Figure 8 — Qualitative illustration of RF ESD design issues with respect to ESD/EMI budget

In very critical design cases, minimizing the “ESD shunt budget” for each component may become a consideration as a way to attain a more desirable position on the Robustness/Performance/Cost tradeoff gamut. Since parasitic capacitance tends to increase with increased robustness in a TVS, a “weaker” TVS component may be chosen to obtain a lower parasitic capacitance that fits within the signal integrity design constraints. In order to maintain equivalent system robustness levels with the weaker TVS component, the component under protection will be required to shunt more of the “ESD shunt budget”, otherwise the achievable overall robustness will be reduced.

For instance, a high-speed serial bus may allow for as little as 1 pF of additional parasitic capacitance on each IO line to pass compliance tests. If that port may be subjected to an 8 kV IEC contact strike, but the physical layer interface (PHY) chip can only tolerate a 2 A peak residual current, then there likely must be some additional external protection added to meet the system level robustness goal. Rather than choose an 8 kV, 1 pF, 0.6 Ohm TVS component that can attenuate the majority of the system level pulse, the system designer may need to choose an 8 kV, 0.5 pF, 1.0 Ohm component that stresses the application specific integrated circuit (ASIC) closer to its maximum limits (Note again, as in Table 2, that while both TVS components might be “rated” at 8 kV, their effect on overall robustness and signal integrity in the system may be radically different due to their dynamic clamping resistance (R_{dyn}) and other parameters).

6.1.4 ESD/EMI Budget Strategy (cont'd)

In this manner the “ESD shunt budget” is shared more efficiently between the two components (see Figure 8C). It is important to understand that this very critically allocated ESD budget should be contemplated in the most restricted circumstances. If the ESD pulse penetrates deep into the system (See Figure 8A) then secondary upset effects are more likely, meaning that there could be a secondary spark inside the system or at least the ESD return current on the ground plane that will generate additional noise effects.

This is analogous to a total distributed insertion loss budget for an inline EMI filter, where two filter components in series both contribute to the total budget. While the two filters could share the attenuation equally or in any arbitrary fraction, the majority of the EMI attenuation should occur in the elements closest to the connector to avoid “polluting” the interior of the system with interference.

Likewise, the ESD protection should be implemented as in Figure 8B, where TVS and filters are placed as close to the IO port as possible and the ESD is returned out of the board as soon as possible.

Both the EMI and ESD budgets are thus optimized by minimizing the overall design margins for the system. This potentially makes the system more vulnerable to both EMI and ESD; therefore this method should be utilized in only the most critical situations.

6.1.5 Equipment Ground

The ESD charge must be stored or returned in a manner that does not affect the operation of the system. This aggressor charge may be safely conducted along the perimeter of a metal product case to an alternating current (AC) mains ground line, or it may charge the volume between a laptop and a tabletop as shown in Figure 9. But it may also charge an IO input gate capacitance beyond its breakdown voltage, or it may be transformed into enough heat by an ESD clamp to permanently damage it.

Again, the overall ability to gracefully transfer or transform ESD charge without damage or functional degradation depends on a good system level path from the system to the outside world. What must be considered are the discharge paths from the system entrance point, to the different local ground nodes, to the PCB ground, to the case ground and to the reference ground of the system level test.

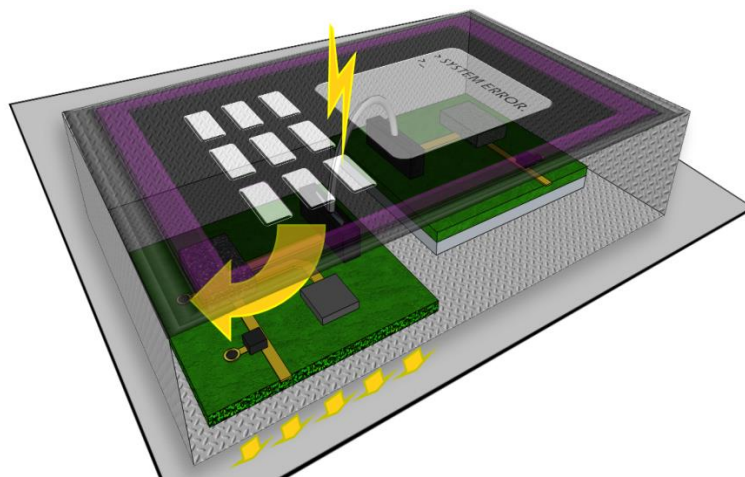


Figure 9 — Discharge path into a keypad, through the system to a local ground, then through the case on the system return path (of a generic device as shown here)

6.1.6 Quick Fixes

Even the best trouble-free legacy designs may suddenly exhibit an unexpected susceptibility out of the designer's control due to user application environment changes, unavoidable supply chain substitutions, end-of-life component revisions, or component variation interactions not anticipated during system design.

In this case, the immediate engineering problems for the designer are to “fix-what-we-have”, and fix it fast! Unfortunately, this problem is resolved through the same design-for-robustness exercise applied during normal product development and design, except that the designer is now constrained to the existing board and components already committed to the supply chain. In this case, an “add-on” component may be the only hope to avoid complete redesign of the system board, if not the entire system. Again, the more information the designer has on failure and suspected “upset vector,” the more accurately he can focus his solution options.

Some options include:

1. Enhancing shielding/grounding with copper tape or improved bonding of conductors, fasteners, product covers, cases and gaskets or other components.
2. Populating “depop” TVS footprints with additional clamping components if the pads were included initially as an insurance policy.
3. Upgrading the components to more robust (potentially more expensive) versions in the same footprint
4. Software recovery methods (catching and correcting ESD upset vectors, see Section 6.2.8)
5. Absolute last resort: Reduce qualification ESD level. (Often not possible for a given application.)

6.1.7 Information Available to the Designer

As described above, little helpful system ESD protection information is provided by component suppliers. System designers may consider external shielding as a first step. While placing a roll of copper tape on top of a laptop is not going to degrade the system ESD robustness, it is the skillful application of such tape/shielding, in the right amount and location, which can actually improve the robustness. Likewise, reactively adding TVS clamps on an IO may not help with the problem at all, and ironically may even make some system ESD problems worse.

System test qualification standards are universally accepted (and required for regulatory purposes, see Annex A for examples) for various applications. However, as shown in Table 2 previously, a uniform test and measurement reporting regimen is not commonly adhered to by component vendors for components that comprise those systems.