

Charvaka Duvvury *Independent ESD Industry Consultant, Texas, USA*

1.1 Definition of Co-Design

Whenever "System Level ESD (electrostatic discharge)" is mentioned, the overwhelming presumption is that it is the design strategy for protection to ESD events by a system manufacturer, while the system designer would not need to understand or comprehend the ESD protection of the component IC itself, which is purely considered as a yield/reliability/manufacturing issue. In deference to this, the system designer applies various methods on the printed circuit board (PCB) and other measures at the End System to meet system ESD threats. The original equipment manufacturers (OEMs) assume that if an IC fails within the system, the ESD performance of the IC itself must be intrinsically weak and hence an improved on-chip ESD robustness should alleviate the situation. But at the same time, the OEMs generally tend to consider that the IC suppliers have an inherent responsibility to ensure a proportion of the system ESD reliability by building in high ESD robustness as a starting point on the chip itself. **COPY THETT CONDUCT CONDUCT CONDUCT**
 COPY COPY TO THE THE AND ANDEL THE AND ALLET AND A THE RESPONDED AND AND A THE SUPPOSED THE THE MEASSIGNED CORPORT OF SUPPOSE THE THE RESPONDIBLE THE CHIRD (THERIC IS THE MATH CORPOR

While these general aspects have mostly been correct for the past few decades, the changing scenarios of technology advances are making it very difficult to continue these practices. To promote a more efficient ESD protection methodology while still ensuring system performance with minimum impact, this book introduces the concept of "Co-Design" to be a more prevalent term in the industry. We simply define *co-design* as an objective to achieve *efficient and harmonized system level ESD protection* with a consolidated effort between the *OEM and the IC supplier*, and more practically as well as critically between the *system designer and the IC ESD designer*.

The intention of this book is to provide all of the background and knowledge of system level ESD and to describe in detail how co-design can be applied to achieve ESD reliability of electronic devices and components.

System Level ESD Co-Design, First Edition. Edited by Charvaka Duvvury and Harald Gossner.

^{© 2015} John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd.

2 System Level ESD Co-Design

1.2 Overview of the Book

Semiconductor component designers and the system designers who integrate those components into a functional product face dramatically different engineering challenges and constraints. Rather than a competitive or isolated vertical development approach, this book proposes system co-design as a cooperative methodology between these two stages of product development in which end-product performance, robustness, and overall cost are simultaneously optimized in the appropriate area for the targeted application environment.

As part of this strategy we introduce system efficient ESD Design (SEED), which defines a particular co-design methodology that deals with the ESD transient characterization and protection of systems, circuits, and devices as an integrated ESD environment, rather than considering isolated subsystem components individually. This concept allows for optimized prevention of permanent ESD damage or temporary product failures, through comprehensive design simulation.

This book aims to introduce the reader to the importance of a SEED-based co-design strategy in the context of changing product markets for a wide variety of electronic applications. What ESD threats and challenges are faced, how the system level protection is approached, who in the supply chain is responsible for providing it, and what is changing in the industry about these strategies will be addressed in detail. From this new perspective, the ideal roles of the IC designer and the system designer will be outlined.

The details of the organization of this book and an overview of the important issues covered in each specific chapter will now be outlined.

1.3 Challenges of System Level ESD Protection

ESD protection continues to be a major challenge for the electronics industry at many different levels. During the production, handling and testing of the IC chips the human body model (HBM) (ESDA, 2012) and the charged device model (CDM) (JESD22-C101C) are important test methods to ensure yield and reliability. However, these requirements no longer apply for the same IC chips once they are implemented into systems (cell phones, laptops, etc.) and require instead to be tested with the system level ESD test, as defined by the (IEC, 2008). Also, in the automotive environments there are other protection requirements (ISO, 2008; RTCA, Inc., 2007). There is scant information on how to efficiently implement system level ESD protection, which often leads to ad hoc solutions that may not be practical or that may interfere with the system operation.

1.4 Importance of System Level Protection

Generally, when electrostatic charge is rapidly transferred between two objects of different potential it is known as an ESD event. In these cases the initial charge voltages can be from 1 V to 35 kV and the discharge currents can reach as high as 60 A during transitions of nanoseconds or even picoseconds. Depending on the events, there are various methods to protect against these ranges of ESD threats. The two standard protection requirements are component level and system level. The scenarios for the two are shown in Figure 1.1. Note first that unassembled components should face much lower ESD threat levels because they are handled in a controlled manufacturing environment. These details are discussed in Chapter 2. A component within a

Figure 1.1 Overview of the component and system level ESD event scenarios. With proper ESD controls as required, the IC devices do not see higher than 1 kV at the most, while in the external environments the ESD pulses can be much higher in magnitude and thus require a good system level ESD strategy

system, on the other hand, can be exposed to much harsher ESD events. The IC pins that are exposed are called "External" or "Interface" pins and the IC pins that are not exposed are called "Internal Pins." With the exception of any externally exposed pins, the IC inside the system is generally safe, as long as proper system level protection is designed. For the exposed pins, an efficient approach for overall system protection requires an understanding of the optimum strategy. The details for this will be covered later.

System level ESD events as described above are depicted in Figure 1.1. When subjected to ESD events, the system may experience "soft" or "hard" failures. So-called soft failure refers to a system lock-up or temporary data loss, while hard failure refers to irrecoverable system damage. Some sources of system ESD include charged humans, charged humans with metallic tools, charged cables, and charged metal objects. These events are transmitted to a system either by a direct contact to the input/output (IO) pin (exposed) or to the system case. An indirect transmission can also occur through a vent hole to the circuit board. Indirect ESD can also relate to pickup of electromagnetic (EM) radiation or a secondary discharge within the system. Many of the details of these phenomena are covered in the later chapters.

Similar to component level ESD testing, a qualification test is also needed for the system level ESD to ensure that finished products can continue normal operation during and after a system level ESD strike. The International Electrotechnical Commission (IEC) has established a standard known as the IEC 61000-4-2 as a test method to represent a charged human holding a metallic object and discharging to a point in the system. Although this is a worst case scenario it is accepted as a standard to assess a system against ESD. Manufacturers of electronic products widely use this method to test a system against ESD. The test actually involves two different types: contact discharge and air discharge. The direct discharge (or contact discharge) simulates ESD into the system, whereas the indirect discharge (or air discharge) simulates ESD close to the system. Most commonly, contact discharge is used as it tends to be relatively more reliable as well as being fairly repeatable. The testing in either case is performed with the system powered on, so that any soft failures as well as hard failures are discerned.

Component IC ESD has traditionally received much focus as a concern for semiconductor production area handling and for maintaining yield. But advances in semiconductor technology for high performance circuits have placed a burden on both component and system level protection strategies. While the component ESD issues are being addressed with changes toward more realistic levels and with much better static control methods in production areas, these improvements do not help reduce system level ESD vulnerabilities in any way. This problem gap continues to grow due to rapidly increasing numbers of electronic consumer and medical products in more widely varied and hostile environments.

There are many different component ESD testing methods used in the electronics industry today. HBM and CDM testing have been used for many years to determine the robustness of ICs to the stresses they may encounter in the manufacturing environment. These stresses are fairly well understood, and methods of protecting ICs from these stresses are well known.

The most challenging part of the system ESD is the magnitude of the pulse relative to HBM or CDM of the component test. This is shown in Figure 1.2, where the different ESD events are compared for their relative magnitudes. The HBM pulse at 2 kV has much smaller peak current, while the CDM at 500 V, although of higher current magnitude, has a very short pulse width (*<*1 ns) and does not represent much energy.

Also shown for comparison are the cable discharge event (CDE) and the electrical overstress (EOS). The destructive EOS events can last as long as a few milliseconds and thus cause massive physical damage to an IC. There is no standard test for EOS as it is often caused by misapplications (Kaschani and Gärtner, 2011). CDE events would represent discharge from charged cables. For example, cables could acquire electrostatic charge primarily due to triboelectric charging, and when the charged cable is plugged into electronic equipment a substantially high energy pulse could occur. This would require the electronics inside to be protected. During a typical test on the interfacing Ethernet pins a cable (∼100 m long) is charged to about 1–2 kV and then shorted at the other end. The resulting waveform is shown in Figure 1.2. The actual rise time for the CDE could be much faster than indicated. Note also that the pulse length for the CDE will depend on the cable length. Protection against cable discharge is a challenge, and selection of an appropriate transformer will modify the residual pulse coupled directly to the IC pin. The ESD designer can then design an on-chip protection to handle this coupled energy. However, EOS pulses can come from many different sources and often require an understanding of the root causes in terms of misapplications, uncontrolled current and voltage spikes, and hot plugging conditions. transient latch-up (TLU) and some otherwise survivable ESD events can also cascade into catastrophic EOS failures.

Figure 1.2 Comparison of different ESD events. HBM and CDM are component ESD pulses; cable discharge and EOS are other types of ESD events; and system level ESD is represented by the IEC standard. Note that the x-axis is not to scale

Although not represented in Figure 1.2, there is another ESD event that is of major concern called the charged board event (CBE). This event occurs when a charged board is plugged into a system, and any discharge event experienced by the interface IC pins would see a very severe form of CDM-like event, typically of 20–30 A magnitude. There is no published standard, nor an established industry accepted IC pin protection requirement presently for CBE. A most effective and practical method to minimize this threat is to use proper control methods during board assembly and testing.

While the above ESD or ESD-like threats are important, the focus of this book is exclusively the nature of system level ESD which we define with the general IEC test method. As seen in Figure 1.2, for the typical IEC system level stress of 8 kV pulse the current magnitude is nearly 30 A, and the secondary portion of the total pulse has a long discharge time similar to HBM but at much higher current than for 2 kV HBM. The IEC curve actually appears as a combination of CDM (initial pulse) and HBM pulse (secondary pulse) with a long decay time. The energy under the IEC pulse makes it difficult to design on-chip but can be done with large clamp devices that can absorb several kV of HBM stress levels. But as will be discussed in Chapter 4 this method is neither practical in general for the ESD designer nor is it necessarily advantageous or efficient for the system designer.

1.5 Industry-Wide Perception

There is often a confusion between the component ESD protection requirements and the system level protection performance that is expected to depend on the component level robustness. The common misconception is that by designing for very high component ESD levels robust protection can be obtained when these devices are in a system. However, as demonstrated in Figure 1.1, the system level robustness measurement is relevant only when the IC is placed on the PCB and is not correlated with the IC component's ESD levels such as HBM and CDM. Besides the IEC testing, there is also strong evidence that real-world system failures are not correlated to their standard ESD ratings (Industry Council, 2010). There are several reasons for this. For example, real-world failures occur in a powered system, whereas component ESD testing is done in unpowered conditions. Also, the current paths are different for the two tests. Adding to this confusion, real-world failures are most often soft failures, which can only occur in system testing or in the field during use, and no amount of ESD testing on the components could comprehend all the possible upset vectors of integration into a system of unknown interconnects and functionality.

A study by the Industry Council on ESD Target Levels (Industry Council, 2010) has shown that for products tested with HBM and IEC test methods there was no correlation between the results of the two methods. This is represented in Figure 1.3 (Industry Council on ESD Target Levels, 2010). Clearly the HBM performance is no indication of its IEC level. This complete miscorrelation comes from the fact that the two tests are characterized by different stress waveforms, and the manner in which the tests are applied is different. However, it must be noted that in some cases external IC pins with higher IC level ESD robustness may make effective IEC design requirements easier but this is not always the case. So, generally speaking one should not rely on the IC pins' HBM and/or CDM performance for IEC protection design.

Therefore instead of focusing on increasing the component ESD levels, the strategy for system protection should instead be based on other factors such as using external clamps and optimizing the board components. IEC (2008) defines another, system level, stress. While this

Figure 1.3 Failure levels for products characterized with both HBM and IEC pulses. Six case studies performed by the Industry Council on ESD Target Levels (WP3PI) are shown here. In all cases the failures were hard failures (Industry Council on ESD Target Levels, 2010)

Figure 1.4 Schematic of an effective system protection method involves two-stage protection to absorb the predominant energy at the TVS device and board components to protect the internal IC pin

stress is intended to be applied to completed products, as product size shrinks the pins of ICs become more closely connected to entry points for this system level stress. As shown in Figure 1.4, transient voltage suppressors (TVSs) of various types capable of withstanding the system level stress are connected to the stress points IC at the board level in an attempt to protect the IC.

But what it is more important – but also difficult – is the implementation of the TVS device to protect the system. A TVS device alone can withstand the system pulse but it does not mean that it will protect an IC pin connected directly in parallel with it. The overall effectiveness depends on the electrical characteristics of both the TVS and the IC pin (Marum *et al.*, 2009). For example, see Figure 1.5 which shows that with an external TVS there is still a voltage applied to the interface pin which it must survive. This is referred to as the "residual pulse" (Dunnihoo, 2005). The nature of this pulse should be understood to formulate an effective protection strategy. SPICE based simulations (Lou *et al.*, 2010) can be helpful to design the

Figure 1.5 The concept of "residual pulse" as described in Marum *et al*. (2009). A TVS device alone cannot protect the interfacing IC pin since the voltage build-up of this device at high currents can still damage the internal pin (S. Marum, J. Watson, C. Duvvury, "Effects of Low Level IEC 61000-4-2 Stress on Integrated Circuits," International ESD Workshop, Lake Tahoe, CA, May 2007.)

right amount of parasitics so that the residual pulse peak current is lower than the failure current for the IO pin under ESD conditions. Without such an approach, the concept of the residual pulse can be misunderstood. This could lead to a confusion about what level of IC pin component protection is required when designing the system level protection.

This concept is better illustrated in Figure 1.6, where the simulation results (Bertonnaud *et al.*, 2012) show that a TVS device alone cannot always protect the internal IC pin. In Figure 1.6, the TVS plus PCB curve indicates the true nature of the residual pulse. Even this might be higher than the interface pin can withstand. In such cases filter elements with corresponding proper impedance to further reduce this pulse have to be implemented. The details

Figure 1.6 Simulated waveforms from (Bertonnaud *et al*., 2012) showing the IEC pulse shape with and without the TVS device. Note that TVS alone still has a large peak that would not protect the internal IC pin. Adding the parasitics of the PCB will mitigate this pulse shape (S. Bertonaud, C. Duvvury, and A. Jahanzeb, "IEC System Level ESD Challenges and Effective Protection Strategy for USB Interface," ESD Symposium Proceedings 2012.)

require more careful design to match the frequency response of the protected pin such as for USB 2 (universal serial bus) (Bertonnaud *et al.*, 2012). Also, these discussions only pertain to hard failures, whereas soft failures require even more complicated issues. The various strategies for both hard and soft failures are presented in the later chapters.

1.6 Purpose and Motivation

There has been a persistent misunderstanding about system level ESD protection, as to who is responsible for its proper design. This can often lead to the expectation that the IC supplier should ensure that all should be safe when their products are placed in the customer's system. But this is not trivial where the system/board designers may not have knowledge of the interfacing IC pins' behavior under ESD conditions. Without considering such aspects, the system protection design may not be optimum. The purpose of this book is to raise all the critical issues for system level protection. These include a clear understanding of the nature of system failures and the methods for efficient protection. To achieve this, better communication is required between the IC supplier and the system builder. This book therefore focuses on what is referred to as system efficient ESD design. There are many complex considerations for system level ESD protection, and this book intends to present this information as well as promote a wider use of the SEED method.

Overall, this book aims to combine the collective knowledge of system designers and system testing experts and summarize the state-of-the-art issues and techniques for efficient system level ESD protection with minimum impact on the system performance. All categories of system failures, from hard to soft, will be considered to review the simulation and tool applications that can be used. The focus of this publication is to define and establish the critical importance of co-design efforts from the IC supplier and the system builder, and to review some practical methods to achieve this objective.

1.7 Organization and Approach

The book is organized into ten chapters with nine different contributing authors. The authors constitute system ESD consultants, industry experts with component and system design solutions, university professors with knowledge in system level ESD simulation tools, and industry members with hands-on experience for system ESD in consumer, mobile, and automotive applications. The condensed information presented here supports the positions of two recently published white papers (Industry Council, 20120; Industry Council 2012) from the Industry Council on ESD Target Levels. We aim to present the most relevant information from the white paper documents and to provide more recent information.

The following chapters will provide detailed nuances of systems, different phenomena that need to be understood, and the development of advanced simulation techniques that should be employed.

Chapter 2 provides a full background of ESD control and IC component protection requirements and methods. The chapter elaborates on why ESD control in the manufacturing line is important for producing reliable ICs that eventually go into system applications. All forms of known ESD threat will first be summarized. Then, important strategies for countering these threats will be outlined, starting from the wafer level, on to packaging, and then to shipping the ICs before their eventual placement in the systems. Next, the standard components test

will be reviewed to describe their critical requirements to ensure that the ICs are safe at the handling stages. The current status of the revised component ESD target levels will also be reviewed to illustrate that the IC performance is a critical function limited by additional protection, and requires realistic goals for component protection levels. This background is given before delving into the actual system protection standards and requirements.

Chapter 3 begins by presenting an overview of system level ESD stress testing as it is presently done in manufacturing facilities and independent test laboratories for the purpose of ensuring compliance with a wide range of standards, both internally driven for product reliability and externally driven by industry or international regulations. These internal and external forces for ESD testing are discussed and lead to an in-depth description of the most widely used test standard for ESD (IEC, 2008). A large portion of this chapter will focus on the details of this IEC standard and how it has influenced subsequent standards development for ESD. Detailed information is presented to show how – and more importantly why – testing in some industries varies from that documented in the IEC standard.

The chapter concludes by describing methods and new technologies that can provide invaluable information to the engineer tasked with determining the root cause of an upset or failure. These new technologies include methods for localizing and in many cases, pinpointing devices and circuits sensitive to becoming upset as the result an ESD event.

Chapter 4 introduces the co-design concept of SEED. First there is a review of the IC on-chip component protection approaches and the impact on IC speed and performance for critical applications such as USB and HDMI (high definition multimedia interface). The chapter then gives more details of the contrast between component level chip protection and the on-chip protection approach for meeting system level protection for the interface pins. This is followed by specifics of what on-chip system protection is, and how it is implemented to meet certain requirements. The advantages and the disadvantages of this direct approach are reviewed before describing the features of off-chip system level protection, including PCB design methods. This background information forms the basis for the description of SEED in more detail where characterization and the modeling methods of ICs and PCB discrete components both for hard and soft failures are presented. The simulation approach for optimizing the system protection using these models is outlined, and the limitation of soft fail characterization is highlighted.

Chapter 5 describes how systems can be protected from physical damage from ESD stresses (hard failures) which enter through system connectors such as power connectors or IO ports such as audio, USB, or HDMI. The chapter opens with a brief description of how sensitive electrical components such as ICs can be damaged by ESD. This is followed by a general discussion of the use of on-board circuit elements to protect ESD sensitive devices and how this can be done by either limiting current or limiting voltage with unidirectional, bidirectional, and breakdown, triggered, and snapback (crowbar) devices.

The characterization of TVS and other types of protection devices is then discussed both in terms of their protection properties and also the quiescent in-circuit properties they need to have during normal operation of the circuit. The quiescent properties are considered in terms of working voltage, leakage, and resultant signal integrity. The ability of TVS devices to survive ESD stresses are explained in terms of ESD simulator gun stress and the human metal model (HMM) standard practice documents. Characterization of TVS devices using transmission line pulses (TLPs), both 100 ns TLP and very fast transmission line pulses (VF-TLPs), is explained, as is the importance of these tools for understanding the effectiveness of a protection device for protecting sensitive circuit nodes, and how they can be useful in studying the properties of

10 System Level ESD Co-Design

sensitive ICs. Characterization of TVS devices with non-HMM pulses such as lightning and other transient pulses (IEC61000-4-5 and IEC61000-4-4) is briefly discussed and contrasted.

Descriptions are then given of the different voltage limiting protection devices which are available and their usefulness or unsuitability for use in ESD protection applications including gas discharge tubes, thyristors, spark gaps, metal oxide varistors, polymers, glass ceramic, and the dominant silicon based protection devices including integrated series-shunt and new ultra low capacitance devices for high speed applications.

The concept of primary and secondary protection is then defined within the SEED concept. TVS devices may form the primary protection, and the protected circuit may be the secondary protection, while the current limiting properties of the circuit board can help in ESD protection. Finally there is a discussion of considerations when choosing protection devices and the use of the SEED when designing the protection strategy.

Soft failures and PCB protection measures are discussed in Chapter 6. As defined in this text, a soft failures leaves no physical evidence. They can be triggered by only a small fraction of the energy delivered to the device under test (DUT) by a typical ESD event. As many weak coupling paths can be found in a system, it is difficult to identify which of the many potential coupling paths triggered the soft failure. Additional complications to the characterization and prevention of soft failures include: (i) soft failures observed in ESD testing with slightly different conditions, (ii) field failures due to software or other problems incorrectly attributed to ESD, or vice versa, and (iii) a lack of industry qualification and standard definitions for soft failures.

In the light of these limits, this chapter provides guidance on the characterization of ICs and boards for their soft-error robustness and different types of soft errors, it shows modeled soft error scenarios, and it illustrates some possible countermeasures. While not as comprehensive as the SEED method for modeling hard errors, a systematic approach is proposed for understanding and handling ESD induced soft failures.

Chapter 7 presents specific design application examples for mobile applications. First, the nature of ESD protection in mobile devices is introduced. In mobile devices the grounding point and grounding path are not always self-evident or as easy to identify as in fixed installations.

In today's extreme focus on cost, the optimum solution is not always possible to implement. This chapter provides several examples where optimizations in one area have created a penalty in another place. The co-design methodology in this text suggests a comprehensive design perspective to resolve such a dilemma.

The mobile section considers the cases of a totally floating device and a simple wire connected device. The optimum shielding solution is introduced with its benefits. Then the ideal mechanical solution and theory is contrasted with practical implementation concerns and real-world constraints. Particularly in mobile designs where ideal shielding is not possible, the concepts of fast ESD and slow ESD become important. As the ESD currents are routed and dissipated around and away from susceptible areas, their effect on the system depends on where these currents are guided and how they are filtered by the shielding. One special part of this chapter addresses some examples and considerations of software- and firmware-based solutions to ESD soft failure symptoms. Some basic design guidelines are proposed for addressing soft failures. Some of these examples prevent software errors in the system, and some examples suggest software-based ESD problem-solving techniques.

Chapter 8 focuses on automotive applications with an explanation of the reasons for the relatively high automotive robustness requirements. Sample EOS/ESD/latch-up signature examples on failing field return circuits are demonstrated as justification for these target levels, and then protection concepts are described to protect the ICs from such damage. A co-design methodology is then described for matching the clamping devices on-board and on-chip in terms of transient turn-on time and clamping efficiency. Depending on the application, for example, basic light emitting diode (LED) drivers or high-speed FlexRay transceivers, the speed of the communication signals is very different and requires different approaches to the design.

For safety applications the integrity of the communication links must be maintained in very critical, noisy situations; GND shifts and failures of individual components on a signal bus must not disturb the communication of the remaining components. These special requirements are widening the voltage range of special interface pins, which are usually going off-board and therefore need to be robust to high ESD levels.

To meet these constraints it is very important to understand the system in which the IC will be used, and to match the solution on the IC with the external TVS diodes integrated on the board. This requires a well-defined module and system specification, software tools for system simulation and IC tools for automated frontend (simulation) and backend (verification) checking. Some examples of ESD/EOS testing are given to optimize the integrated solution and to verify the parameters according to specification. Finally some important guidelines are provided to prevent common failures and to ensure a safe launch of a device for automotive applications.

Chapter 9 presents the future issues for extension of SEED for system level protection into the next decade. First, the models for simulating the system level need to be understood for their limitations and what aspects need to be considered to further refine them. Many advances are expected in advanced high-speed systems which will continue to drive the system protection design into conflict with the performance demands. These will all lead to burden and challenges for system protection. These issues will be presented in the context of providing benefits and a perspective for the next generation of systems and their continued requirements for ESD protection.

Finally, Chapter 10 addresses the problem of balancing the ideal ESD robust technical solutions available against the real-world constraints of cost and performance. A conceptual three-way continuum "co-design gamut" is presented to help conceptualize the interacting dynamic trade-offs between price (or cost), performance (or quality), and robustness (or susceptibility).

The optimum overall system trade-off point is described in more detail between these three primary constraints. This system optimization goal may differ dramatically depending on the perspective of the IC or PCB designer in the vertical product chain. The final system vendor who ships the product under their brand name and end-user warranties may have a considerably different threshold requirement for robustness than a CPU or peripheral IC designer who is primarily focused on squeezing every last bit of performance out of a technology in controlled lab environments. Here the concept of co-design is applied to optimizing the design goals between these two (or more) perspectives, and this may be impeded by corporate "siloing" or partitioning of design groups even within the same nominal company.

Beyond the design community, this chapter also encourages manufacturing, marketing, and management to develop an appreciation of and understanding for the limitations and

constraints of engineering by considering the end business opportunity costs of asking for too much of one specification, or not enough of another. This idea is then extended to the experience of the end users, who hold the ultimate market-driven verdict on the product's success, and who are unfortunately likely to have the least amount of relevant data informing their decision. It is this point at which all decisions from prototype to production must converge and align with the final customer.

Finally, this chapter considers the product co-design development cycle beyond a single product iteration to multiple product cycles and numerous application usage models. Over time, and in different applications, the trends required in specifications and design goals for the trade-off gamut can be identified and predicted. Many times, these trends converge in the worst possible way. For example, higher performance and higher integration devices enable wider application venues, continuously exposing increasingly susceptible technologies to ever more perilous environments and failures.

1.8 Outcome for the Reader

This book is directed toward industry ESD designers, system integrators at OEMs and original design manufacturers (ODMs), and both quality and operations management professionals of IC suppliers and their direct customers.

IC suppliers often face additional difficulties in meeting customer ESD demands on their IC chips, and having a clear understanding of the techniques presented here should enable them simulate and remedy the scenarios far more effectively and offer better solutions that do not compromise the system performance.

This book will also serve the academic education needs on the subject, especially for professors and graduate research students. The book is provided as a reference for both the basic learner and the specialist in the field.

Acknowledgments

Grateful thanks are offered to Jeff Dunnihoo for many of his helpful comments, and to all of the other authors Robert Ashton, Harald Gossner, Michael Hopkins, David Pommerenke, Pratik Maheshwari, Wolfgang Reinprecht, and Matti Uusumaki for informative summaries of their respective chapters.

References

- Bertonnaud, S., Duvvury, C., and Jahanzeb, A. (2007) IEC system level ESD challenges and effective protection strategy for USB interface. ESD Symposium Proceedings 2012.
- Dunnihoo, J. (2005) Protecting the HDMI Interface. EE Times (Jul. 16 2005), http://www.eetimes.com/documents .asp?doc id=1273577 (accessed 04 November 2014).
- ESDA/JEDEC ANSI ESDA/JEDEC JS-001-2010. (2010) *ESDA/JEDEC Joint Standard for Electrostatic Discharge Sensitivity Testing – Human Body Model – Component Level*, ESDA/JEDEC.
- HBM Test Method introduced by ESDA and JEDEC in 2011. Currently ESDA ANSI/ESDA/JEDEC JS-001-2012. (2012) *Joint JEDEC/ESDA Standard for Electrostatic Discharge Sensitivity Test – Human Body Model (HBM) – Component Level*. HBM Test Method introduced by ESDA and JEDEC in 2011.
- IEC 61000-4-2. (2008) *Electromagnetic Compatibility (EMC) Part 4-2: Testing and Measurement Techniques – Electrostatic Discharge Immunity Test*, www.iec.ch. (accessed 01 November 2014).

- ISO Standard 10605. (2008) *Road Vehicles Test Methods for Electrical Disturbances from Electrostatic Discharge*, International Organization for Standardization.
- Industry Council on ESD Target Levels. (2010) White Paper 3 System Level ESD Part I: Common Misconceptions and Recommended Basic Approaches, December 2010, www.esda.org (accessed 31 October 2014) or JEDEC publication JEP161. *System Level ESD Part I: Common Misconceptions and Recommended Basic Approaches*, www.jedec.org (accessed 31 October 2014).
- Industry Council on ESD Target Levels. (2012) *White Paper 3 System Level ESD Part II: Implementation of Effective ESD Robust Designs*, 2012, www.esda.org (accessed 31 October 2014) or JEDEC publication JEP162. *System Level ESD Part II Implementation of Effective ESD Robust Designs*, www.jedec.org (accessed 31 October 2014).
- JEDEC Standard JESD22-C101C. (2004) *Field-Induced Charged-Device Model Test Method for Electrostatic-Discharge-Withstand Thresholds of Microelectronic Components*.
- Kaschani, K.T. and Gärtner, R. (2011) The impact of electrical over stress on the design, handling and application of integrated circuits. Proceeding of the 33rdEOS/ESD Symposium, Anaheim, September 11–16, 2011.
- Lou, L., Duvvury, C., Jahanzeb, A., and Park, J. (2010) SPICE simulation methodology for system level ESD design. Electrical Overstress/Electrostatic Discharge Symposium Proceedings, pp. 65–73.
- Marum, S., Duvvury, C., Park, J. *et al*. (2009) Protection Circuits From the Transient Voltage Suppressor's residual Pulse During IEC 61000-4-2 Stress. Proc. EOS/ESD Symposium, 2009, 377–385.
- RTCA, Inc. (2007) Environmental Conditions and Test Procedures for Airborne Equipment, DO-160 rev. F, RTCA, Inc., June 2007.