



June 2018 – Sept. 2018 • Volume 10, Issue 2 (Published since 2009), April 30, 2019

Compendium Special Edition on Electrostatic Discharge (ESD)

Damage from ESD is a major cost to the microcircuit industry in terms of time, money, and mission risk. The *EEE Parts Bulletin* has released three special issues on ESD, and this issue is a compendium of these three issues plus an overall view of the subject matter. The first issue dealt with the need to upgrade specifications related to ESD and suggestions for better ESD practices wherever parts are manufactured, stored, or prepared for shipment. The second ESD special issue focused on a parts failure investigation that ultimately concluded that ESD was the most likely cause of the failure. The second issue also included an important reminder about regular ESD testing. The third issue provided an example demonstrating the importance of maintaining ESD discipline and a high-level risk analysis related to electrostatic discharge. This compendium issue begins with an overview of the subject of electronic parts and ESD. Figure 1 provides a reminder that the familiar static sparking from rugs or rubber combs can generate ESD effects. ESD damage can easily go undetected.

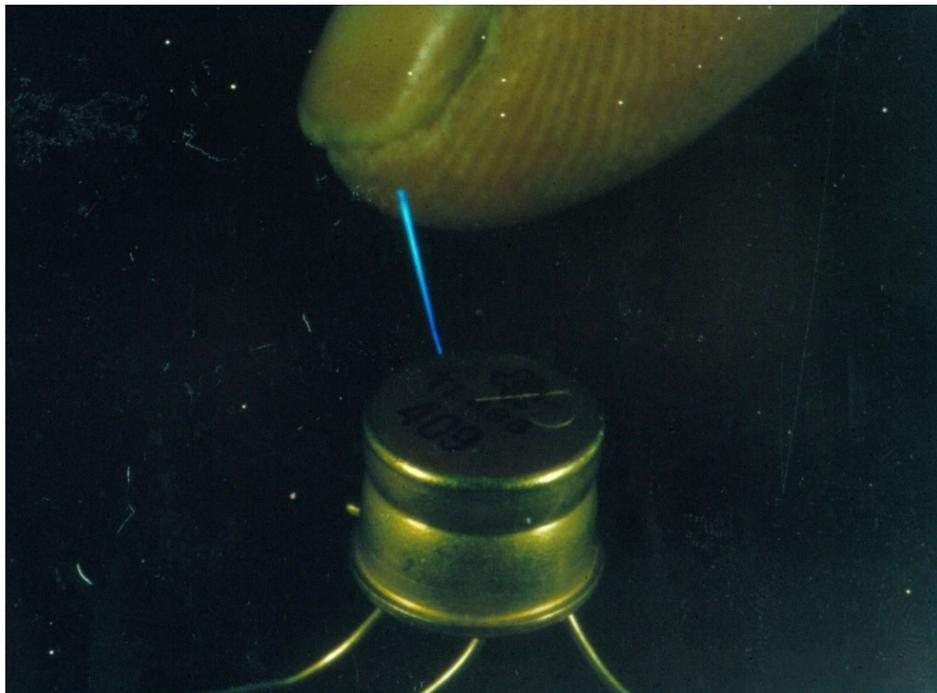


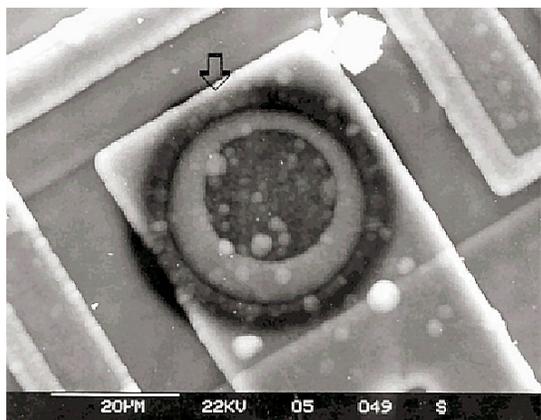
Figure 1. Electrostatic discharge is everywhere (image courtesy of Hi-Rel Laboratories).

Gaps and Mitigation Strategies for ESD

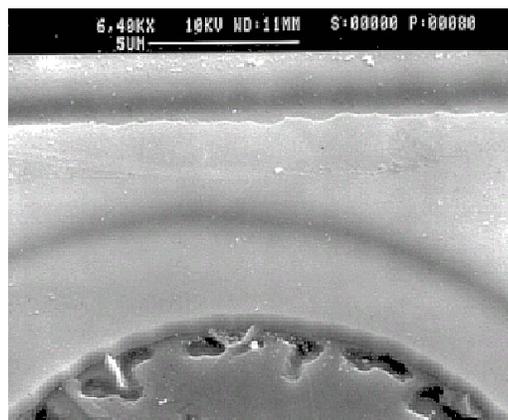
Progressively smaller and more complex microelectronic parts have grown steadily more susceptible to ESD. Consequently, they require more testing effort.

Furthermore, ESD damage can easily be too small for detection by many typical methods. As Figure 2 shows, serious ESD damage can be invisible to optical viewing and even to 6400 X by scanning electron microscope (SEM). In this instance, only a 33,000 X SEM view made the damage visible.

Damage Is Not Optically Visible



Not Visible at
6400 x In SEM



Damage Visible at
33,000 x In SEM

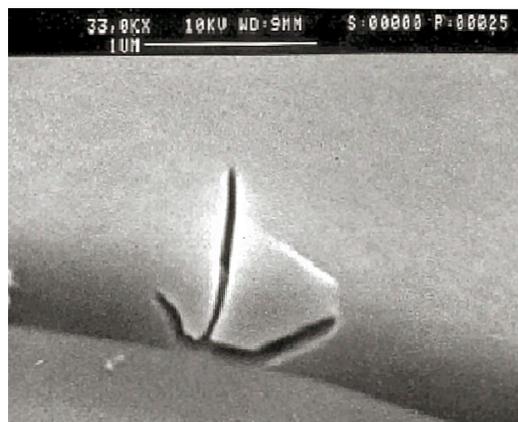


Figure 2. ESD damage to most semiconductors is often so subtle that it cannot be seen without very high magnification (image courtesy of Hi-Rel Laboratories).

Such ESD damage affects all types of commodities for both military and commercial parts, and the less-controlled commercial-off-the-shelf (COTS) parts may be affected more severely than the military.

The parts community must promote an ESD-safe environment. Such efforts must extend from parts fabrication, through shipping, and all the way through installation of parts in the final products.

NASA has supported this effort first by bringing ESD concerns to the attention of the parts community. Mitigation strategies have been developed in response to this rising threat. Mitigation strategies include NASA ESD surveys, observations during audits, standards updates (including harmonization of standards), and outreach to the military and space communities.

NASA has been supporting Defense Logistics Agency (DLA) audits of the supply chain for many years. During the audits in recent years, the auditors observed that the MIL-PRF-38535 requirements were practically non-existent regarding ESD aspects of electronic parts.

Hence, integrating ESD requirements into MIL-PRF-38535 has become a key goal for the electronic parts community. The current qualification standards for MIL-PRF-38535 and related standards were developed years ago with pin counts in the twenties. Now, pin counts are in the hundreds or more. For instance, Virtex field-programmable gate arrays (FPGAs) have 1752 columns, and manufacturers are striving for even higher counts.

Applying the old device testing standards to modern high-pin count products can cause severe problems. Testing times and costs can increase dramatically. However, costs also drive the need for adequate quality assurance. Per-unit prices for advanced devices are approaching \$200K, and the costs would multiply for failures discovered after a part was mounted or (worse) was in the field... or worst of all, in space.

Another issue is that multiple organizations have developed ESD mitigation standards/specifications. Gaps have evolved not just because of new technology, but also because of inconsistencies of standards development.

For the military and space community, the most glaring issues are as follows:

MIL-STD-883, Test Method 3015 Issues:

- Too old
- Does not include the charge device model (CDM), only the human body model (HBM)
- The test method needs to be revisited for smaller feature sizes down to 30 nm.
- The test method needs to be revisited for large numbers of contacts/pins, and vastly increased

time to test, and advances in packaging (e.g. 2.5/3D, also known as stacking).

MIL-PRF-38535, Performance Specification for Microcircuits:

- Poor coverage for ESD (no CDM testing required).
- The MIL-PRF-38535 Rev L, which is under review, says in 4.2.3, Electrostatic Discharge (ESD) sensitivity, that ANSI/ESDA/JEDEC JS-001 for Human Body Model (HBM) as an alternate to MIL-STD-883, Test Method 3015. These two should be compared to identify differences and make them consistent. For instance, they contradict with Test Method 3015 specifying testing three electric pulses (zaps) per pin and JS-001 specifying two zaps per pin for the human body model (HBM) test.
- Needs to be updated for new technology and for shipping and handling of products in multi-supply chain production of parts (which is becoming the norm).
- Must specify that ESD requirements do also apply to wafer foundries.
- Take a new look into the ESD behavior of high-speed pins.

NASA ESD Mitigation Going Forward in FY2019

NASA is continuing the effort to lead and/or support ESD efforts in the following categories:

- Continuing to perform NASA ESD surveys.
- Making independent evaluations of new technologies (e.g., high speed and high power microcircuits, GaN devices, SiC devices). Characterization of ESD thresholds per Human Body Model (HBM) and Charged Device Model (CDM) for new devices.
- Characterizing new packaging technologies (e.g., 2.5D and 3D) as they become available for HBM and CDM.
- Performing independent evaluations of 883 vs. JEDEC test method equivalencies for HBM.
- Developing low-ESD-threshold parts mitigation, e.g., GaN, very high speed ICs (GHz range)—conduct limited tests to make recommendations.

- Continuing to conduct NASA ESD surveys.
- Interfacing with industry standards groups (e.g., JC-13, JC-14, ESDA, EC-11, EC-12).
- Working especially with the JC-13 newly-formed task group to address ESD issues. [JC-13 defined in the bullet above—just added standards.]
- Harmonizing ESDA 20.20, JEDEC 625, and other ESD standards.

Final ESD Reminders

- ESD is a serious and growing risk for electronic parts use.
- Updated standards are coming, and they will help mitigate ESD risks.
- However, the most important point to remember is that mitigation of ESD risk requires continuous vigilance in identification of risks and discipline in maintaining safeguards.

References

ANSI/ESDA/JEDEC JS-001-2014, ESDA/JEDEC Joint Standard for Electrostatic Discharge Sensitivity Testing—Human Body Model (HBM)—Component Level.

ANSI/ESD S20.20-2014, Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices), Electrostatic Discharge Association, 2014.

JEDEC 625, Requirements for Handling Electrostatic-Discharge-Sensitive (ESDS) Devices. JEDEC Solid State Technology Association, 2012.

MIL-STD-883K, Test Method Standard, Microcircuits, Defense Logistics Agency, Columbus Ohio, April 25, 2016.

MIL-PRF-38535K, Integrated Circuits (Microcircuits) Manufacturing, General Specification for, Defense Logistics Agency, Columbus Ohio, Dec. 20, 2013. (Revision L is in review).

For more information, contact

Shri Agarwal 818-354-5598

1. First Special Edition on Electrostatic Discharge (ESD)

January–July, 2016 • Volume 8, Issue 1, Revision A, March 14, 2017
Special Edition on Electrostatic Discharge (ESD)
(The NASA *EEE Parts Bulletin* has been published since 2009)

Note: This revision added details and corrects ambiguities in the original issue released Aug. 31, 2016.

Damage from ESD (see Figure 1) is a major cost to the microcircuit industry in terms of time, money, and mission risk. We plan to release two issues. This first special issue deals with the need to upgrade specifications related to ESD and suggestions for better ESD practices wherever parts are manufactured, stored, or prepared for shipment. This issue also included an article about partnering in radiation and reliability testing [deleted for ESD compendium].

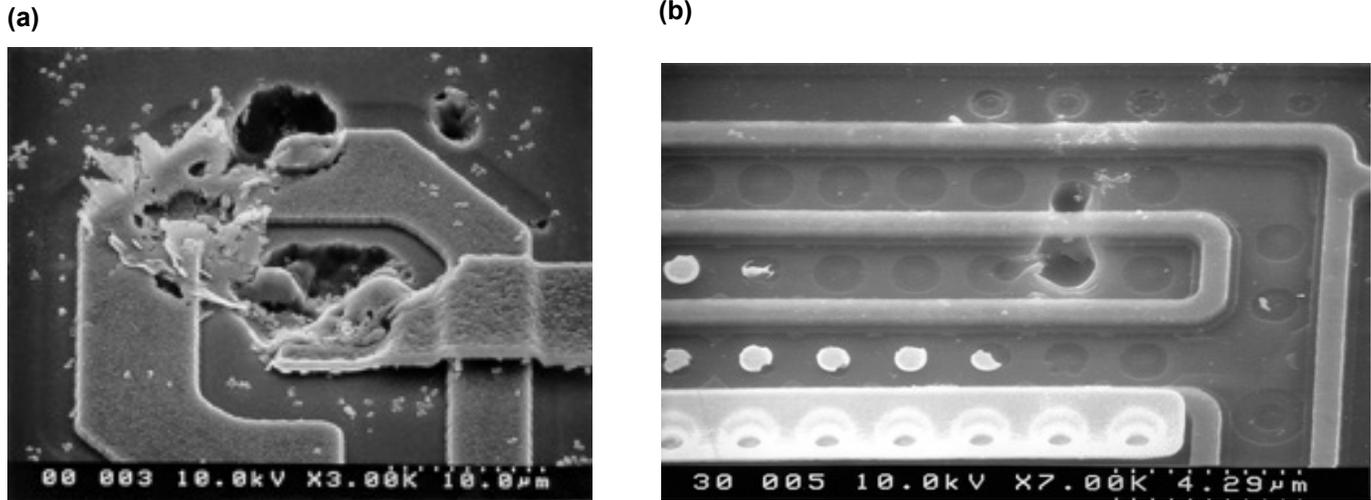


Figure 1. Examples of ESD damage to microcircuits (Images courtesy of JPL Analysis and Test Laboratory):

- a) A static random access memory (SRAM) device with 5-micron features was deliberately exposed to an 8000-volt pulse from a 100-picofarad capacitor. This produced an approximately 5.3-ampere peak current pulse lasting just under one microsecond. Melting of conductive traces is typical of such ESD damage and creates an open circuit path.
- b) An undefined microcircuit with 1-micron line widths that failed in service after being exposed to a pulse of approximately 500 volts. This caused a breakdown of the SiO₂ layer and a short circuit in the part.

Upgrading ESD Control: Its Importance and Possible Strategies

A. What Is ESD and How Are ESD Controls Applied?

Electrostatic discharge or ESD in electronic parts is an electrical sparking event that functions like a tiny version of lightning. When two objects with different potentials are brought sufficiently close, a current flows toward the ground equalizing the potential. These differences can be caused by friction of dissimilar materials (shoes on a carpet is a classic example), but even the difference in potential between a human body and an object may be enough to initiate an ESD event.

For electronic parts, built to carry minute amounts of current, tiny lightning bolts are a cause for concern. If such an errant current flow of an ESD goes along the outer case of a part or the outside of an ESD-resistant (anti-static) bag or shipper, there may be no problem. However, if such a current goes through the part, serious damage may result. ESD damage can include catastrophic damage and/or latent damage. Catastrophic

damage is immediately detectable by the resulting loss of function and often visible damage. Latent damage is not immediately detectable because there is no loss of function and often no visible sign of damage. However, the part has been weakened and may fail in the field or (worse) in space.

This has always been a serious concern for electronic parts, but it has grown steadily more urgent.

The purpose of this article is to sensitize the entire space community, and in particular, the standards-developing-bodies to the fact that the ESD requirements must be clearly specified in such standards documents so that everybody handling microcircuits, from manufacture to final use can minimize ESD damage. Furthermore, the standards must be updated to reflect the present level of technology.

In this context, the role of DLA (Defense Logistics Agency) for the department of defense (DoD) becomes vital. The standardization branch of DLA develops and maintains the military (MIL) standards, which are used for maintaining high-reliability quality parts production for the

DoD and for NASA. Also, manufacturers and non-MIL standards organizations provide inputs to the standards

These standards are often enforced by periodic audits of parts manufacturers and their supply chains. The audit branch of DLA officially conducts enforcement. NASA actively supports DLA in both of these activities.

For the purposes of this article, we are focusing on monolithic microcircuits. The standard most commonly used by the U.S. space community for high-reliability microcircuits is MIL-PRF-38535, Integrated Circuits (Microcircuits) Manufacturing, General Specification for. Any microcircuit parts produced under the military system must be in compliance with the requirements of this document.

The 38535 is the periodically changing overall document controlling microcircuit quality and reliability. The ESD aspects of the document clearly need updating. For auditing, the requirements must be flowed down to the working audit, and it must be reflected in each manufacturer's quality management (QM) plan.

Also, the ESD-related standards used by other organizations may provide ideas for upgrades to the MIL standards. Conversely, it would be highly beneficial if the MIL standard upgrades were coordinated with other standards bodies so that practices throughout the industry might be as similar and interchangeable as possible.

B. Why Improved ESD Control Practices Are Crucial

Designers have improved microcircuit performance in two ways: smaller size to allow more circuits per unit area (parts densification) and higher operating speeds. (See ESD Technology Roadmap, for more detail on these trends [1]).

Moore's Law has continued with microcircuit densification down to less than 50 nm for many components and some components at 20 nm and less. That and advancements in packaging technologies have resulted higher pin counts to accommodate highly complex microcircuits (e.g., system on a chip).

In the last decade, pin counts have increased particularly for communication and computing products. NASA and the space community are using 1752-pin counts, and higher counts are growing more common in the general market.

Furthermore, some applications use not just smaller parts but parts that need to operate at speeds of 1, 10, even 30 gigabits per second (Gbps).

The improved performance attained by increasing parts density and higher speeds has come at the cost of greater sensitivity to ESD. Thus, it becomes increasingly important to implement better methods of controlling potential damage from ESD. A wide assortment of books and journal papers provides information on methods for mitigating ESD.

A related issue is that current ESD rating methods were developed with typical pin counts in the twenties. Applying these old device testing standards to modern high-pin count products can cause severe problems. Testing times increase dramatically. Worse, wear caused by repeatedly stressing the same path and the increasing influence of tester parasitic losses (parasitics) can lead to false-positive failures.

For high-reliability microcircuits (where a part may cost as much as tens of thousands of dollars), organizations often develop and enforce required policies and procedures designed to mitigate ESD. These policies and procedures are codified in standards.

Furthermore, the landscape of microcircuit part production, handling, and shipping has changed radically. Because of the increased complexity of parts, the paradigm of a manufacturer shipping directly to a customer has largely given way to a highly dispersed production environment, which in turn, often requires highly dispersed ESD control among a number of organizations. Table 1 shows all the steps at which production or use of a microcircuit might be done by shipping to another facility. (The most extreme cases of maximum dispersion are more likely with new products such as flip chips.) Moreover, each of the steps involves at least one environment each for working on the part, storing the part, and shipping the part to the next step in the production.

Table 1. An Extreme Example of possible dispersion of production for a microcircuit product.

Company	Operation/Use
Component Level	
A	Die design
B	Wafer fabrication
C	Wafer bumping
D	Package Design
E	Assembly
F	Column attach
G	Testing and screening
H	Radiation testing
I	Transport by a franchised distributor
J	User Inventory Operations
K	Kitting of upper-level assembly operations
Board Level and Above	
L	Board-level test and verification
M	Intermediate board-level assembly

Company	Operation/Use
N	Final box-level assembly
O	Placement of the box level assembly containing the part in a system (e.g., aircraft, spacecraft, or appliance)

Note: At board level and above (L–O), reduced ESD failures can be realized through upper-level design mitigation (usually electromagnetic interference (EMI) compliance and spacecraft charging mitigation) and also box-level handling processes. System-level handling processes can also reduce occurrences (for example, shorting plugs and connector covers) for the integration and test phase of the electronics system.

Increasing the number of shipping steps in the supply chain increases the number of points where ESD damage may occur. All this needs to be quantified.

It is important to recognize and fully address all the risk points to which ESD sensitive parts are subjected: from when they are fabricated and delivered from the original component manufacturer’s (OCM) site; through supply chain avenues to user inventories; then on to kitting and upper-level printed circuit board (PCB) level assembly, test, and verification; and eventually to final box level assembly, test, and final system level test. This is particularly important for handling, packaging, and shipping of ESD Class 0A devices (<125 volts in the Human Body Model). (See ANSI/ESDA/JEDEC JS-001-2014, ESDA/JEDEC Joint Standard for Electrostatic Discharge Sensitivity Testing – Human Body Model (HBM) – Component Level, listed in subsection D).

C. Questions Related to Upgrading ESD Control Requirements

This section of the article describes challenges of high pin-count ESD device testing, solutions, and possible future trends in the standardization of device testing.

Some issues to consider include:

- What are the differences and the advantages vs. disadvantages of the MIL standards, the JEDEC standards, the ANSI/ESD standards, and other standards for potential use and/or which might influence the MIL standards?
- Are all three commonly used ESD models still valid or should the standards focus on one or two models? Those models are 1) human body model (HBM) based on people accumulating electric charges; 2) charged device model (CDM) based on materials becoming charged after they rub against other materials; 3) machine model (MM) [designed to simulate a machine discharging through a device to ground].
- Do we want a standard for reducing the number of pin combinations required for testing?

- Would statistical pin testing be a good approach?
- How can the testing time be reduced without losing useful information (and significantly impacting the test data)?
- Should the MIL standards be expanded to include charged device model (CDM) testing?
- How do the new 2.5D and 3D configurations affect ESD testing? (See Electrostatic Dis-charge (ESD) in 3D-IC Packages [2]).

We need to consider future trends when revising test standards. This issue is growing more important because the unit costs of contemporary devices are very high (and are growing costlier as more functionality is added), on the order of several tens of thousands of dollars per unit. Poor ESD environment for such products creates possibility of damage/ latent damage to them, both of which could be very expensive. Costs for implementing an ESD-prevention program are miniscule compared to the overall cost incurred in dealing with ESD damage.

The above concerns were presented by NASA representative Michael Sampson at the June 2016 SAE SSTG-12 Space Subcommittee meeting. He proposed that the military documents that control the ESD requirements for testing and rating ESD event severity be reviewed and updated as a first step. As part of this update process, he suggested that the Defense Logistics Agency (DLA) Land and Maritime, which serves as the qualifying authority to maintain the MIL system of parts qualification, perform an engineering practice (EP) study on ESD to detail these issues and compare possible specification changes with those being implemented or proposed by other organizations, in particular, the NASA Inter-Agency Working Group related to ESD (NASA IAWG-ESD). Ideally, coordination among the various standards-setting organizations would result in updated ESD standards with a great deal of commonality. DLA shared the results of their EP study at the JEDEC meeting held in January 2017. Based on the EP study and responses to it, JEDEC (JC-13) has opened a task group to resolve issues related to ESD.

These document changes will require review and coordination with associated reference documents from other organizations to bring consistency.

D. Existing Standards That Contain ESD Control Requirements and Suggested Changes to Them

As noted earlier, the Department of Defense MIL system has an extensive set of ESD requirements and related documents. In addition, several other standards organizations have existing ESD-control requirements documents.

The listing below includes some of the most important ESD standards relevant to MIL devices.

MIL-STD-883, Test Method Standard, Microcircuits, Rev. K, U.S. Department of Defense, April 25, 2016

- Test Method 3015, “Electrostatic Discharge Sensitivity [ESDS] Classification”

<https://landandmaritimeapps.dla.mil/Programs/MilSpec/ListDocs.aspx?BasicDoc=MIL-STD-883>

MIL-STD-883 includes Test Method 3015 (TM 3015), “Electrostatic Discharge Sensitivity Classification,” which establishes the procedure for classifying microcircuits according to their susceptibility to damage or degradation by exposure to ESD. This test method utilizes what is called the human body model (HBM) and it was developed many years ago.

Unfortunately, MIL-STD-883/TM 3015 has not kept pace with the new technology developments. It needs to be revised for the new technology features, such as smaller size, greater numbers of pins, and advanced packaging as mentioned earlier.

MIL-STD-1686, Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices), Rev. C, U.S. Department of Defense, Oct. 25, 1995.

The MIL-STD-1686 is the central MIL document that relates to ESD-related material in other documents, such as test methods. Because this document is widely referenced, it needs to be updated because it has not been revised since 1995.

SEMI E78-0309, Guide to Assess and Control Electrostatic Discharge (ESD) and Electrostatic Attraction (ESA) for Equipment, Semi International Standards, July 2008.

MIL-PRF-38535, Integrated Circuits (Microcircuits) Manufacturing, General Specification for, U.S. Department of Defense, Dec. 20, 2013,

<https://landandmaritimeapps.dla.mil/Programs/MilSpec/ListDocs.aspx?BasicDoc=MIL-PRF-38535>

Paragraph A.4.4.2.8, Electrostatic Discharge Sensitivity, states that, “ESD classification shall be done in accordance with TM 3015 of MIL-STD-883 (the testing procedure defined within JESD22-A114 may be used as an alternate with acceptable correlation data) ...” (See discussion below under E, Correlation.)

MIL-PRF-38535 has no specific ESD requirements for wafer foundries. However, Test Method (TM) 3015 of MIL-STD-883K and SEMI E-78-0309 constitute ESD classification methods to specify the sensitivity level for appropriate packaging/handling requirements and wafer manufacturing equipment. The entire section does not relate to laboratory practices, but it is important to note that they are a critical component of electronics needing ESD control, and perhaps a new ESD standard for the aerospace and defense community should address that.

Suppliers on their own take precautions but there is nothing in the specification to audit to. For example, the ESD properties of fousps (boxes used to carry wafers during processing) may degrade over time.

JESD22-A114F, For Electrostatic Discharge Sensitivity Testing Human Body Model (HBM) - Component Level, JEDEC Standard, JEDEC Solid State Technology Association, Arlington, VA. The JESD22-A114F has been superseded by the ANSI/ESDA/JEDEC JS-001 series of standards. However, some standards may still cross-reference this older standard.

ANSI/ESDA/JEDEC JS-001-2014, ESDA/JEDEC Joint Standard for Electrostatic Discharge Sensitivity Testing – Human Body Model (HBM) – Component Level. This is a revision to the JS-001-2010 document, which merged the JESD22-A114F and another ESD/ANSI standard. (Note: Revisions are denoted by changes in the last four numbers of the document, as in 2010, 2011, and 2014.)

ESDA/JEDEC JS-002 2014, Electrostatic Discharge Sensitivity Testing - Charged Device Model (CDM) - Device Level, August 29, 2014. This standard series is the CDM standard comparable to the JS-001 HBM series. It is also revised by year as denoted in the last four digits of the name.

ANSI/ESD S20.20-2014, Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices, Electrostatic Discharge Association, 2014. S20.20 was prepared by the Electrostatic Discharge Association (ESDA). There are differences between MIL-STD-1686 and this document. Refer to the ESDA website for details.

NASA-STD-8739.7, Electrostatic Discharge Control Excluding Electrically Initiated Explosive Devices. This document was cancelled in December 1997. However, resurrecting it is an option.

E. Correlation or Combining of ESD Documents

MIL-PRF-38535 directs that testing can be done by either MIL-STD-883/TM3015 or JESD22. However, the two documents have differences in their test methods.

- 883, TM3015 states that each device shall be tested using three positive and three negative pulses using each of the pin combinations as shown in Table II in the document. A minimum of a 1 second delay shall separate the pulses.
- Whereas, JESD22 states that each sample shall be stressed using one positive and one negative pulse with a minimum of 300 milliseconds between pulses per pin for all pin combinations specified in table 2 of the document.

The community must consider whether these two test approaches provide the same results and identify

necessary updates to the affected documents. A total review of the documents must be done to find and resolve any other differences.

Several major manufacturers have used other standards to perform tests not included in 38535, for example, using a charged device model (CDM) to characterize the ESD sensitivity level. (For more information about CDM, refer to Electrostatic Discharge Sensitivity Testing—Charged Device Model [CDM]—Component Level, ANSI/ESDA/JEDEC JS-002).

This is a growing issue. As the partial listing of standards in the previous subsection suggests there has been a great deal of work accomplished in developing standards for ESD mitigation, but it has been done by multiple groups. Standards of the various groups have a number of minor and major differences.

These different streams of standards development have caused waste through duplication of effort. Of more immediate concern is that suppliers and users who straddle more than one such group face greatly increased complexity of operations. This increased complexity can increase costs, increase potential supplier–user disputes, and increase the potential for parts failures due to ESD weaknesses in production.

Thus, there can be tremendous benefit by negotiating to achieve “harmonization” of standards. Harmonization can be done in some combination of three ways:

1. Different groups can combine multiple documents into a single document (e.g., combining of standards to generate JS-001-2010, now 2014),
2. Incorporate parallel changes in standards from different groups, and
3. Reference a standard elsewhere as part of one’s own standard or contract (e.g., the military and space community often uses ANSI/ESD S20.20 regarding ESD).

F. Upscreening of Commercial-off-the-Shelf (COTS) and Other Parts

Performing ESDS testing when upscreening parts is not a common practice, but it should be considered by the users. At the June 2016 G12 meeting on plastic encapsulated microcircuits (PEMs), it was reported that manufacturers can lower ESD sensitivity ratings on COTS parts without any notice.

G. Conclusion

We have provided a brief introduction for two issues with ESD in microcircuits. First, the smaller part sizes of parts densification are making microcircuits much more sensitive to ESD. Meanwhile, the increased pin counts allowed by densification are increasing the complexity, risk, and time required for ESD testing on those parts. Consequently, methods for mitigating ESD must be correspondingly upgraded.

Second, there are multiple ESD mitigation standards that have been developed by different organizations. In turn, it is not clear which of these ESD standards are being used by each link in the microcircuit supply chain. This enormously confuses contracts and quality control among different organizations. It would be extremely useful to coordinate the ESD standards to make the requirements as similar as possible and to have them specified in as few standards as possible and include them in MIL-PRF38535.

Third, NASA is in the process of resurrecting the old NASA-STD-8739.7 document on ESD control. This document will unify the Agency’s centers and field component centers and align industry partners with NASA to common control program elements. The resurrected standard will contain a minimal set of built-in quality controls, it will reference industry documents, it will be tailorable and concise, and it will ensure quality workmanship from the component level through system assembly.

References

- [1] *Electrostatic Discharge (ESD) Technology Roadmap*, EOS/ESD Association, Inc., Revised May 2016.
- [2] *Electrostatic Discharge (ESD) in 3D-IC Packages*, Global Semiconductor Alliance, Version 1.0, Jan. 14, 2015.

For more information, contact:

Shri Agarwal 818-354-5598
Gene Monroe 757-864-6156

Typical ESD Weaknesses and Suggested Control Improvements from Supplier Plant Visits

Controlling electrostatic discharge (ESD) is a key component for electronic parts assurance auditing to ANSI/ESD S20.20. In early 2016, two personnel from NASA JPL (Minh Do and Jose Uribe) conducted an ESD survey at a typical microcircuit supplier to identify any ESD issues in the supplier’s operations. Similar surveys at different locations have yielded comparable results.

We would like to share some of these typical results and findings with the NASA Electronic Parts Assurance Group (NEPAG) and the wider electronic parts community. These ESD surveys are usually a result of findings during an audit by the qualifying activity (QA) for MIL standard parts. (This function is performed for the U.S. Government by DLA, and NASA is also an active participant in this function.) Such facilities usually have an ESD program in place, but they can often benefit from equipment upgrades and procedure updates such as:

- a) Employee training. This is critical; and everyone in the work area must be aware of his/her surroundings and be properly trained in the handling

of ESD-sensitive (ESDS) devices. As a confirmation for auditors, the workplace employees shall be trained to the organization's ESD control plan (CP).

- b) A calibrated ESD field meter. This is essential. Analog field meters should be replaced by the newer and more accurate chopper-stabilized digital field meters. Also, the field meters should be calibrated at least annually.
- c) Housekeeping. This is important in keeping potentially static-generating clutter (mainly packaging material) away from an ESDS area (also known as ESD protected area). NASA requires that all static generating material or non-grounded personnel be at least 1 meter (39 inches) away from the ESDS area, in contrast to the ANSI/ESD S20.20, which calls out 1 ft (0.3 m).
- d) Older chairs may need replacement. They often have seating surfaces that do not meet the electrical resistance requirements, so the drag chains or conductive wheels do not work properly. Chairs that do not meet ANSI/ESD STM12.1 electrical resistance requirements should be replaced, particularly for ESD protected areas (EPAs), handling parts with sensitivities less than 125 V (Human Body Model, HBM).
- e) Properly-grounded racks. Be sure that the metal racks used to store or to transport parts between workstations are properly grounded. Rubber or plastic gaskets between metal sections may insulate the sections and prevent grounding (see Figure 2). Exposed ESDS parts cannot make contact with metal surfaces directly; however, they can contact static dissipative materials.



Figure 2. Photograph showing a plastic insulator inserted at each connector junction in a storage rack. Such rings prevent grounding of items stored on the rack. Lack of grounding could lead to build-up of a damaging electrostatic charge. (Figure courtesy of Steve Bolin.)

- f) Resistance measurements often show the groundable points in a facility having different resistances (some as high as several megaohms). Ideally, all groundable points should measure very low resistance (less than 0.1 ohm).
- g) One of the best upgrades for ESD protection is to replace wrist strap testing with continuous wrist strap monitoring. When doing this, it is important to use a system having two wire wrist straps rather than the common single wire wrist straps. Single-wire wrist straps do not allow actual monitoring of resistance to the operator but instead rely on measurement of impedance and can be fooled. Single-wire systems will, in fact, indicate safe grounding of the operator even when an insulating barrier such as a shirt is placed between the wrist strap and the operator's skin.
- h) Also for grounding, workers must affix their wrist straps against their skin rather than over clothing. A wrist strap will fail to alarm if, for example, it is on the sleeve of a person's lab coat.
- i) Belt furnaces or shuttle ovens are always difficult to properly ground due to moving parts, and they are often found to be isolated from the ground or "floating." Using an air ionizer of sufficient capacity near the furnaces will help in these cases.
- j) Old cathode ray tube (CRT) monitors are still occasionally found on wire bonders. The CRTs produce very high voltage static fields. Such CRT monitors should be replaced with flat panel displays (which do not charge) or groundable CRTs. (Both of these types of equipment are commercially available). In the rare cases in which the CRT monitors cannot be replaced, they need to be removed from the ESD protected area or made safe by enclosing them in a perforated metal box and covering the screen with a groundable transparent shield, which shields the parts in the wire-bonding area from the CRT screen.

Reference

- ESD Association Standard Test Method for the Protection of Electrostatic Discharge Susceptible Item, AN-SI/ESD STM12.1-2013 – Electronic, (accessed Oct. 24, 2016).*
- American National Standards Institute (ANSI) Electrostatic Discharge (ESD) Association Standard for the Development of an Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices), ANSI/ESD S20.20.*

For more information, contact:

Jose Uribe
Minh Do
Steve Bolin 818-354-3699

2. Second Special Edition on Electrostatic Discharge (ESD)

August 2016–May 2017 • Volume 9, Issue 1 (Published since 2009), June 16, 2017

Second Special Edition on Electrostatic Discharge (ESD)

This second ESD special issue focuses on a parts failure investigation that ultimately concluded that ESD was the most likely cause of the failure. The issue also includes an important reminder about regular ESD testing and a table of standard microcircuit drawings that were recently reviewed.

Figure 1 is an example of damage that was probably caused by ESD.

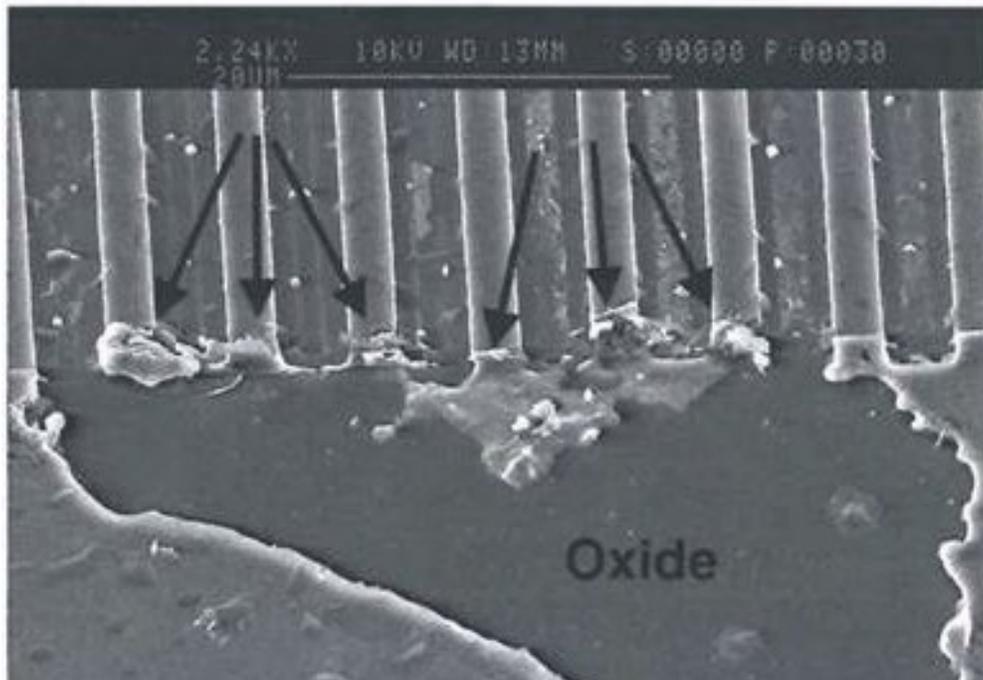


Fig. 1. Detailed view of a damaged site on a metal oxide semiconductor field-effect transistor (MOSFET) probably caused by ESD.

ESD, the Silent Killer

A. Background

There are several important points to consider with respect to ESD knowledge, practice, and compliance. However, the key for ESD program success is consistency. If we detect the results of an event, then, we (the operational group) should be able to ascertain and confirm that we never have any lapses in the program implementation. With systematic practices, we should be able to surmise that there is no way any events can occur on the organizational project watch.

ESD is the silent killer in electronics, and the resulting impacts are hidden project costs that are the motivator to address project risk cost and schedule impacts. When an ESD event occurs, one of three scenarios may occur.

1. There is no impact, and no detrimental result.
2. There is a catastrophic strike and the immediate electronics operation failure is detected, isolated, and repaired. Repairs may be easy or done at great expense, but they are done.

3. The most undesirable event may happen. Undetected damage to one or more parts results in latent defects that are either detected during ground test operations or (worse yet) during mission operations (when any resulting failures may be beyond repair).

The later an ESD event happens in the product life cycle of the system, the greater the project cost for repair. Latent defect end-of-life prediction is weak due to lack of access to flight and in-orbit malfunctioning hardware for analysis purposes.

Under these circumstances, we need the highest possible confidence levels in our ESD program compliance at all times in order to be fully effective.

Part replacement costs not only include part costs, which can range from about \$100 (for a typical active part) to about \$40,000 (for field-programmable gate arrays, FPGAs), but also the repair labor and mission assurance logistics and disposition. The real hidden costs can potentially escalate when considering the diligence to complete “run to ground” root cause failure analysis,

possibly numerous technical/material review boards and completion of all final documentation for disposition of the ESD failure event.

The cost of the labor hours alone associated with all the program/project technical authorities, subject matter experts, and electronics-hardware assembly personnel attending the disposition meetings can in most cases out cost the replacement value of the damaged part alone. Many of these personnel also participate in system tear-down, acquisition of the new part screening/testing of the new part, emplacement of the new part, reassembly, and retesting of the repaired system. Therefore, prevention is a multi-faceted reward.

B. Examples

Below are a few examples of some metallic oxide semiconductor field-effect transistor (MOSFET) devices that were damaged during the assembly of a recent space flight International Space Station (ISS) support instrument box. The parts were received in ESD protective packaging and not removed until board-level assembly soldering took place. The failed board-assembly-level verification and the ensuing troubleshooting ruled out design or operational issues. The suspect parts were removed, tested, and shipped off for failure analysis.

Figure 2 shows the PCB assembly with two noted non-functional parts circled in red. Although not conclusive, the corner location of damaged parts on the board was thought to be important to the forensics analysis. One theory implied that handling of the board (by the perimeter) allowed for the ESD event to contact these parts directly. During transport, the board is handled only inside an ESD-approved materials bag. There were questions as to the integrity of these transport bags. Due to bag traceability and reuse issues, there was no definite conclusion on this concern.

Figures 3 thru Figure 7 Show the die and damage areas from various photographic and radiographic perspectives. During upper-level assembly circuit troubleshooting, the potential for design or operational damaging voltages to the MOSFET gates were conclusively ruled out. The circuit was incapable of generating the necessary damaging voltages that would have the effect observed.

C. Investigation Conclusion

The conclusion of this ESD failure investigation was that failure was attributed to user error but review of all ESD compliance logs showed that all precautions were taken during operator handling. Due to lack of further evidence, the OCM and the PCB assembly operation were not ruled out as possible culprits, but neither could be confirmed.

Under these circumstances the team was advised of the event and warned of the total cost for repair and the need to double check all future handling procedures. The board was repaired with same lot date code parts, and there

were never any repeat operational issues with that PCB assembly nor at the box operational level. The “Silent Killer” only struck once on that program, at least as far as can be determined at this time.

Figures 1 through 7 (provided courtesy of NASA Langley Research Center) were generated by Hi-Rel Labs as part of a project Component Failure Investigation at Langley.

For more information, contact:

John E. Pandolf 757-864-9624

A Reminder That Details Are Crucial for ESD— Example: Heel Straps

Over the course of many years, NEC Corporation of America has conducted audits of a variety of manufacturers handling ESD-sensitive materials, and has seen many issues regarding ESD handling. Many of them are small mundane details; yet, failing to maintain the discipline in performing them can lead to expensive ESD parts incidents.

One type of recurring problem we have seen many times is the misuse of ESD heel strap testers where the testing is conducted with ESD flooring installed. The grounding straps must be periodically tested to be sure their function has not been compromised by being stepped on, caught in doors, etc.

For operators wearing heel straps or conductive footwear on both feet, the proper use would be to place the foot-under-test on the test plate, raise the untested foot from the floor and to depress the test button of the tester. Then, the raised foot is switched to test the grounding of the other foot strap.

It is and obvious and standard procedure, but often forgotten. Audits have uncovered usage where the operator leaves the untested foot on the floor, allowing a conductive path to the floor even if one of the straps is not functional, distorting the test results.

The lesson learned is to go through the tests by the procedures book rather than memory. Forgetting little details can cause big sparks.

For more information, contact

Robin Gomi, NEC Corporation of America

978-758-3703

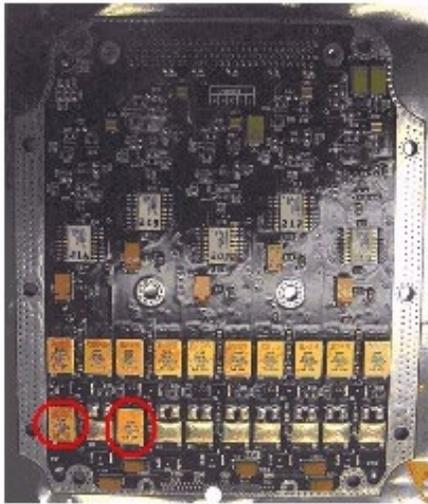


Fig. 2. Damaged parts are circled in red.

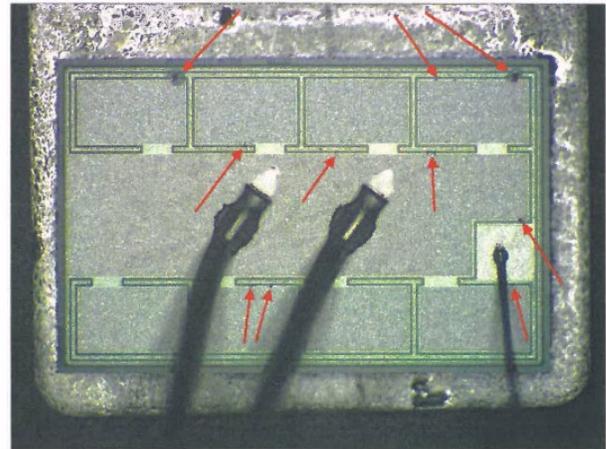


Fig. 3. Optical micrograph of the die in the failed device. The red arrows indicate the damage sites.

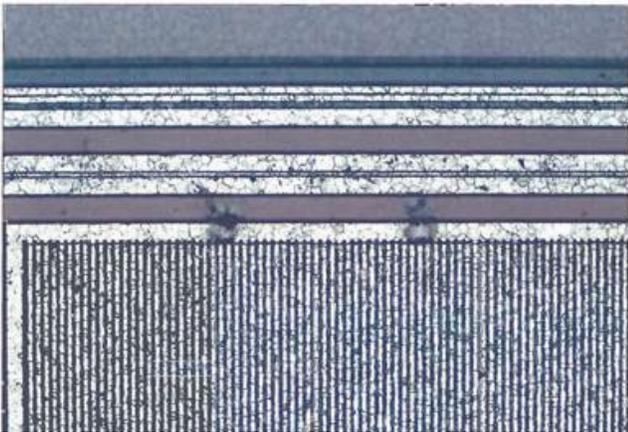


Fig. 4. Detailed view of the damage sites on the die.

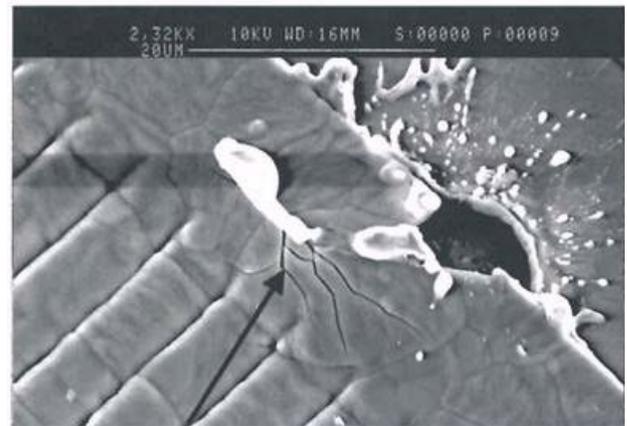


Fig. 5. SEM image of one of the damage sites. The arrow indicates the area where the damage originated

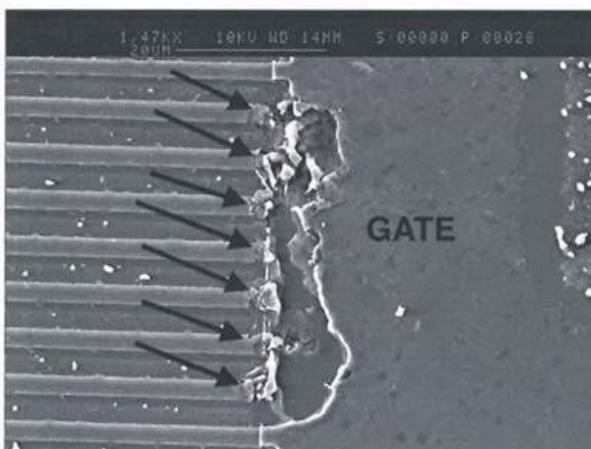


Fig. 6. SEM image of the FET after delayering. The arrows indicate the damage at the ends of the gate runners.

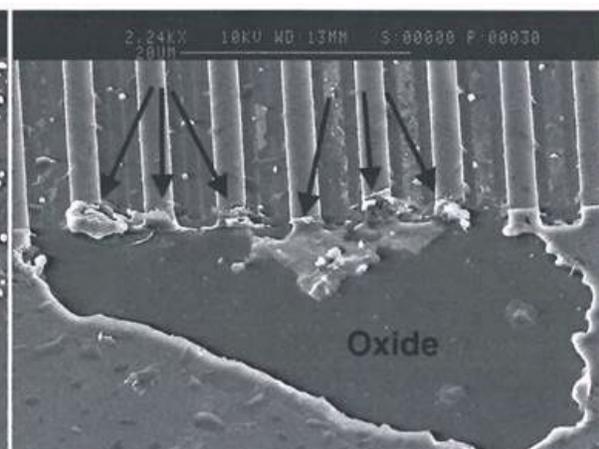


Fig. 7. SEM image of another damaged area on the die. Note that the gate polysilicon fused during the failure, which is why the oxide is visible.

Resistors and Electrostatic Discharge (ESD) Susceptibility

MIL-PRF-55342 resistors are the primary NASA standard for established reliability chip resistors. These resistors are used in a wide variety of mission-critical applications, and will be the main focus of this article. Current knowledge is that passive components such as resistors can sometimes be more sensitive to ESD than active components, which were historically considered at-risk.

Resistors are a technology area where there is a pronounced trade-off of greater capability vs. greater sensitivity. There is no designator for thin film versus thick in the part number, just a temperature coefficient (TCR). Thin films have a low TCR, whereas thick films have higher TCRs. Thin film resistors are much more ESD sensitive than thick films. Thin films can be sold against requirements for all TCR values so all part numbers are assumed to be ESD sensitive even though most high TCR lots are likely to be thick film and quite ESD resistant. ESD precautions should be taken when handling these devices. Field failures of thin-film resistors, in particular, have been attributed to ESD events and have resulted in anything from a few percent deltas in resistance to full open circuit failure.

Per MIL-PRF-55342, Section 6.6: “Under relatively low humidity conditions, some types of film resistors, particularly those with small dimensions and high sheet resistivity materials, are prone to sudden significant changes in resistance (usually reductions in value) and to changes in temperature coefficient of resistance as a result of discharge of static charges built up on associated objects during handling, packaging, or shipment.”

One Manufacturer’s Approach to ESD Mitigation and Control

State of the Art, Inc. (SotA) is one of DLA’s Qualified Parts List (QPL) resistor manufacturers. The following material describes the SotA approach to mitigating and controlling ESD. However, it must be emphasized that ESD practices vary significantly among manufacturers and users. Thus, the ESD practices of other resistor manufacturers may be different from those of SotA.

Table 1 shows SotA thick- and thin-film resistors tested in accordance with MIL-STD-883, Method 3015. ESD sensitivity depends on the manufacturing technology, the case length, and the resistance value.

Table 2. SotA Resistor ESD Sensitivity Classification.

SotA Resistor Technology	Resistor Chip Size	ESD Classification per MIL-STD-1686 (HBM)	ESD Voltage Threshold
Thin Film	0402 and 0505	1C	<2000 V

SotA Resistor Technology	Resistor Chip Size	ESD Classification per MIL-STD-1686 (HBM)	ESD Voltage Threshold
	0302, 0502, 0603, and 0705	2	<4000 V
	1005, 1010, 1206, 1505, & 2208	3A	<8000 V
	2010 & 2512	3B	≥8000 V
Thick Film	0302 & 0402	1B	<1000 V
	0502, 0505, 0603, 0705, & 1206	1C	<2000 V
	1005 & 1505	2	<4000 V
	1010	3A	<8000 V
	2010, 2208, & 2512	3B	≥8000 V

*NOTE: This table and many of the citations herein have been sourced directly from SotA and its publications. It is recommended that you contact your resistor manufacturer for comparable data packs and any relevant ESD precautions.

The MIL-specifications SotA uses to address the sensitivity of resistors to ESD events are as follows.

MIL-STD-1686 addresses ESD control programs and SotA’s full classification of parts, assemblies, and equipment is accomplished by using three defined models:

- Human body model (HBM)
- Machine model (MM) (there is some discussion over whether machine model is still applicable)
- Charged device model (CDM)

MIL-HDBK-263 is the ESD control handbook that addresses ESD considerations for specific components and assemblies and classifies devices as class 1, 2, or 3 (HBM classes) in accordance with MIL-STD-1686. It refers to the HBM test method, MIL-STD-883, method 3015, as the “...the military ESD test method for microelectronics.”

ANSI/ESDA-JEDEC JS-001-2010 and **MIL-STD-883H**, method 3015.8 define the component’s ability to withstand ESD sensitivity classes (Table 2) and the cases matched to sensitivity classes for thin- and thick-film resistors.

Typical Types of ESD Damage Recorded by NASA

According to the NASA Goddard Space Flight Center, testing has shown that imposed ESD damage produces four basic effects: little or no damage, current crowding, internal arcing, and external arcing. They reported it was rare to see all of these effects in the same test network. The following images show ESD damage to resistive film layers (see Figures 8–11) [1].



Fig. 8. Vicinal view of ESD induced damage to a thin-film resistor network chip during ground testing [1].

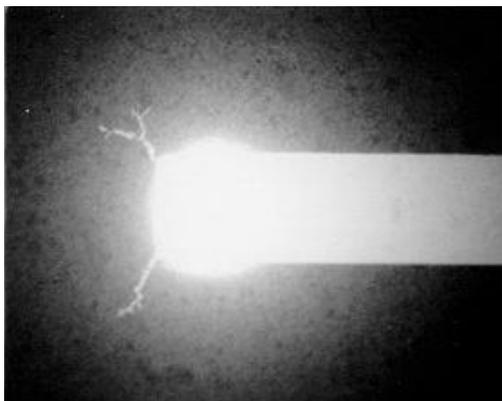


Fig. 9. Vicinal illumination view of corner crowding induced damage [1].

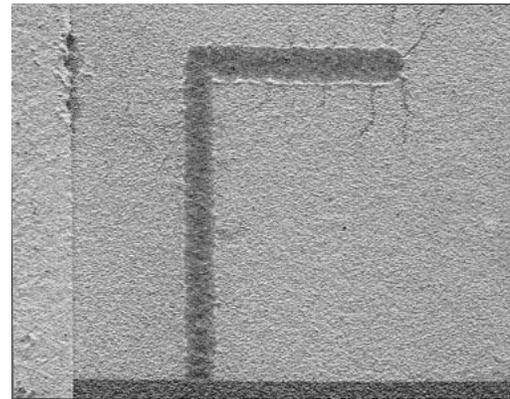


Fig. 10. SEM view of ESD damage in a tantalum nitride resistor. Note the internal arcing damage to the left of the laser kerf [1].

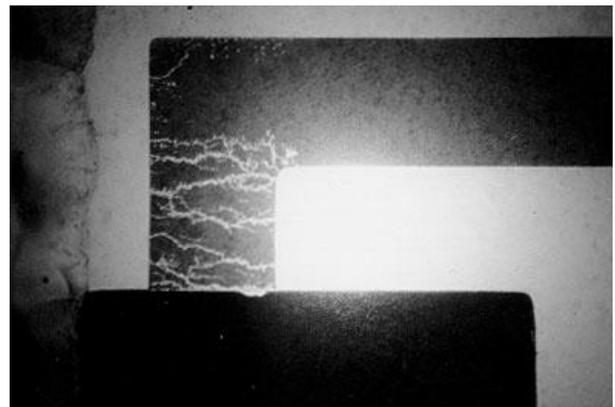


Fig. 11. Vicinal illumination view of transverse cracking typical of relatively high voltage ESD damage [1].

References

- 1) **Electrostatic-Discharge (ESD) Failures in Thin-Film Resistors**, Scott M. Hull, NASA Goddard Space Flight Center, Greenbelt, MD, Jan. 1, 1999. <https://ntrs.nasa.gov/search>
- 2) **MIL-PRF-55342, Resistor, Chip, Fixed, Film, Non-established Reliability, Established Reliability, Space Level, General Specification For**, Rev. H, U.S. Department of Defense, Jan. 29, 2016 <https://landandmaritimeapps.dla.mil/Downloads/MilSpec/Docs/MIL-PRF-55342/prf55342.pdf>
- 3) **MIL-HDBK-263, Electrostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices) (Metric)**, Rev. B, July 31, 1994.

- 4) **MIL-STD-883H, Method 3015.8, Test Method Standard, Microcircuits, Rev. K, Change 2, Test Method 3015, "Electrostatic Discharge Sensitivity Classification"**, U.S. Department of Defense, July 20, 2016.

<https://landandmaritimeapps.dla.mil/Programs/MilSpec/ListDocs.aspx?BasicDoc=MIL-STD-883>

- 5) **MIL-STD-1686, Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)**, Rev. C, U.S. Department of Defense, Oct. 25, 1995.

- 6) **ANSI/ESDA-JEDEC JS-001-2010, Electrostatic Discharge Sensitivity Testing -- Human Body Model**, ESD Association & JEDEC Solid State Technology Association, Jan. 13, 2010. <https://webstore.ansi.org/>

- 7) **State of the Art, Inc. Catalog. CAT# 1628**. <http://www.resistor.com>

**For more information, contact:
Jennifer Hill, 818-354-3290**

We thank State of the Art, Inc. for their willingness to share their information and approaches regarding film resistor device history and ESD test procedures used with these devices.

3. Third Special Edition on Electrostatic Discharge (ESD)

August 2017 – May 2018 • Volume 10, Issue 1 (Published since 2009), July 17, 2018

Third Special Edition on Electrostatic Discharge (ESD)

Damage from ESD is a major cost to the microcircuit industry in terms of time, money, and mission risk. This is the third issue on the subject. It provides an example demonstrating the importance of maintaining ESD discipline and a high-level risk analysis related to electrostatic discharge. Figure 1 shows a major failure caused by ESD.

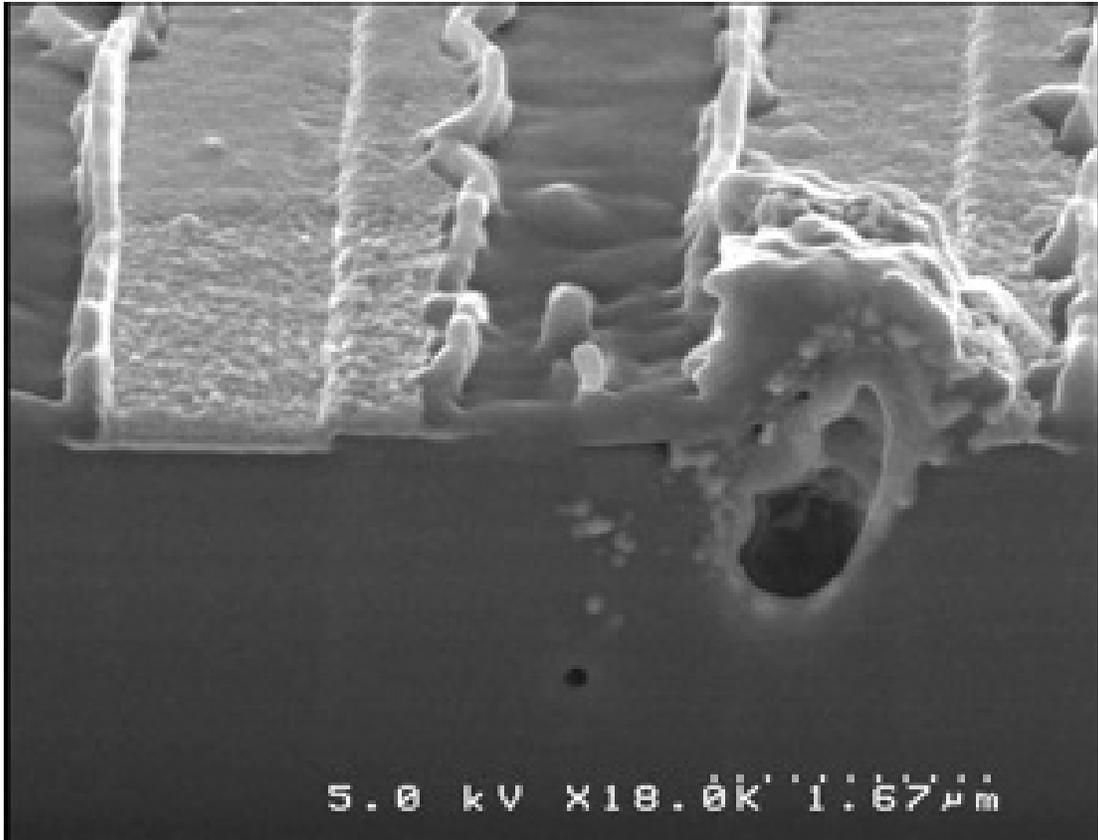


Figure 1. An ESD event of roughly 2.3 kV struck an RF transistor. The current caused a hole penetrating the underlying diffusions and an accumulation of material that re-solidified and shorted between the emitter and the collector (image courtesy of Hi-Rel Laboratories).

ESD Issues and Specification Updates in Progress

Figure 2 summarizes the flow process developed to address major issues such as multiple conflicting ESD standards. In the figure, two paths lead from DLA audits and NASA ESD surveys to eventual changes in standards related to updates in ESD practices. The organizations involved are the Defense Logistics Agency (DLA with its engineering practice studies) in the upper path. The lower path includes the NASA Electronic Parts Assurance Group (NEPAG, with its Government Working Group, GWG), the NASA ESD surveys, and the NASA *EEE Parts Bulletins*. The two paths converge with the findings passed on to the space and military community. The primary community standards organizations are the Society of Automotive Engineers (SAE) and the JEDEC (not an acronym), which have various committees

involved with parts standards. The standards organizations may decide to form a task group to further study issues raised, update existing standards, or develop new standards. The manufacturers (JC-13) and users (SAE, CE-11, and CE-12) meet three times a year to discuss and update the electronic parts standards. The standards organizations provide a forum in which parts suppliers, DLA, NASA, the military services, and other users discuss ways to modify the parts standards and specifications to deal with those issues.

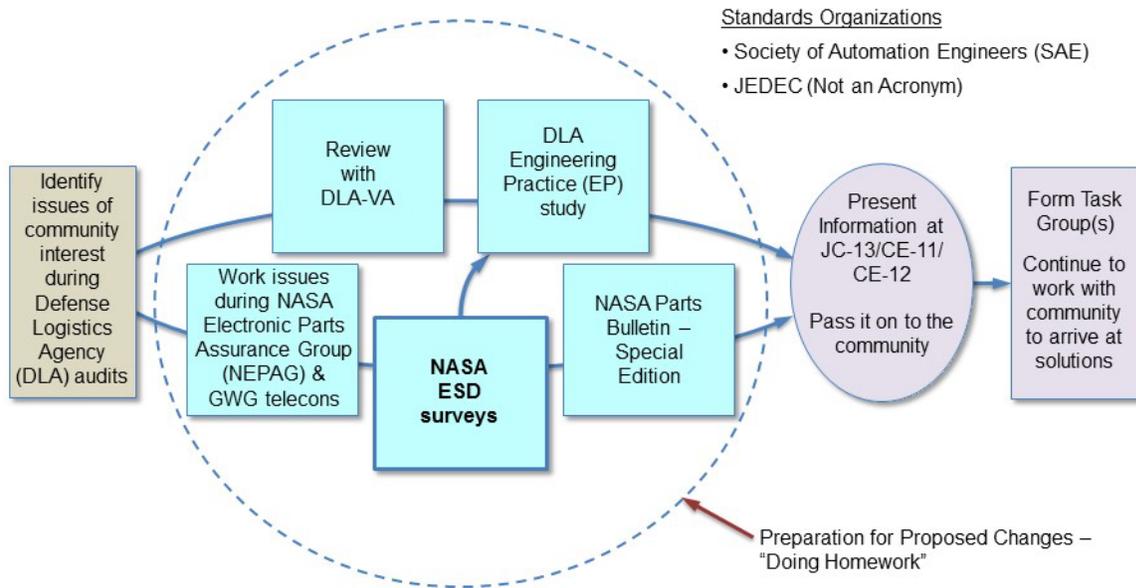


Figure 2. Changes to ESD standards as a sample of how observations from DLA audits and NASA ESD surveys raise issues and how resolutions are developed for those issues.

Some of the concerns raised before the parts community related to the deficiencies in military document MIL-PRF-38535 that need updating are:

- No CDM testing required,
- Confusing requirements (e.g., 883 vs. JEDEC of 3 zaps/pin vs. 1 zap/pin, respectively, for human body model test), and
- It is not clearly stated that the ESD requirements apply to foundries.

Similarly, MIL-STD-883, Test Method 3015 items that need updating are:

- Smaller feature sizes (down to 45 nm),
- Greater number of contacts/pins (previous designs had dozens of pins, now many more, e.g., ~1750 pins for Xilinx FPGA). This greatly increases testing time, and
- Advances in packaging (e.g., 2.5D, 3D) have not yet been addressed.

We need to consider future trends when revising test standards. This issue is growing more important because the unit costs of contemporary devices are very high (and are growing costlier as more functionality is added), on the order of hundreds of thousands of dollars per unit. Poor ESD environment for such products creates the possibility of damage or latent damage to them, either of which could be very expensive. Costs for implementing an ESD-prevention program are miniscule compared to the overall cost incurred in dealing with ESD damage.

NASA is working with the community on electronic parts and ESD. DLA has issued a marked-up version of MIL-

PRF-38535 to Revision L. It includes many updates on ESD requirements. NASA is continuing to perform ESD surveys of the supply chain. There is also an effort to harmonize JEDEC JESD 625 and the Electrostatic Discharge Association (ESDA) 20.20 documents.

Reference

MIL-STD-883K, *Test Method Standard, Microcircuits*, Defense Logistics Agency, Columbus Ohio, April 25, 2016.

MIL-PRF-38535K, *Integrated Circuits (Microcircuits) Manufacturing, General Specification for*, Defense Logistics Agency, Columbus Ohio, Dec. 20, 2013.

For more information, contact:

Shri Agarwal 818-354-5598

Lessons Learned on the Importance of ESD Training and Hardware Access Limitations for CubeSat-Level Projects

In order to minimize the chance of an electrostatic discharge (ESD) event occurring and damaging hardware, it is extremely important to keep hardware access limited to those experienced with ESD precautions and/or trained to ESD control standards such as ANSI S20.20.

An example of this manifested on a small project using a comparably small supplier. The project was a six-unit CubeSat, a 20 X 30 X 10 cm spacecraft, that was deployed from the International Space Station (ISS) with a short mission duration of 90 days.

Although only a CubeSat with a cost of less than \$10 million, it still used a number of sophisticated components, many of which came from suppliers to the CubeSat industry. On such small projects, many people wear multiple hats, and this extends to CubeSat subsystem suppliers. Most of these suppliers do not have a certified quality management system (QMS); rather they are often start-ups with limited experience.

The best suppliers are near QMS level and can be expected to perform tasks without additional support. The suppliers with lesser capabilities may need ESD guidance and support.

In this CubeSat project, one of the small suppliers was a software development group providing a subsystem for this CubeSat. This software development group needed access to the lab to test software. However, software developers are not always as experienced with handling flight hardware as those who are more intimately involved with the integration and testing of said hardware. Under management and schedule pressure, the software developer was given a large task needing regular access to hardware, but was not sufficiently instructed as to the hardware's ESD sensitivity or the ESD controls required.

The project provided an electronics board to the subsystem supplier for this testing, and during this testing the board ceased functioning. The root cause was not explicitly determined, but follow-up investigations strongly suggested that ESD controls were not properly exercised by the software developer during testing. One individual admitted to not wearing a wrist strap while powering hardware on and off. The training and experience of these individuals in the area of ESD controls was clearly insufficient. This lack of controls probably resulted in major hardware damage causing significant schedule and budget impacts to the project. Possibly, the damage could have been prevented if the subsystem had processes for training such lower level teams and monitoring their access to the hardware.

Three valuable lessons were learned. First, a project should survey or otherwise check the ESD practices of all subsystem suppliers. Second, that surveying activity should extend to the lower-level teams or individuals who may also need access to the hardware in addition to all regularly considered assembly and test personnel. Finally, a project should instruct their supplier to upgrade ESD practices if necessary and possibly even provide support in doing so.

Reference

ANSI/ESD S20.20-2014, *Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)*, Electrostatic Discharge Association, 2014.

For more information, contact:

Amanda Donner 818-393-8636

A Risk Analysis Related to Electrostatic Discharge and Other Failure Mechanisms

A. Failure Reports Analyses and Results

The data analyzed for this study originated in failure reports spanning a period from January 2001 through September 2013. These reports are created when a system development project requests the failure analysis lab to perform a detailed analysis of a failed electrical component.

Background information for each is included describing the situation that led to the failure (e.g., failed a visual inspection or electrical testing). Occasionally, detailed information regarding the assembly history is included; for example, an incident occurring at initial power up or following environmental or electrical testing, or a unique situation such as testing following a component repair/replacement.

A total of 283 reports were reviewed. Data from 232 of these reports were categorized for this analysis. The remaining 51 reports described instances where the initial failures during system testing were not confirmed at the failure analysis lab. Situations where this could have occurred include undetected defects in the component mounting (e.g., an improper solder joint that was no longer present after the component was removed) or an intermittent fault. Figure 3 shows the number of failures that occurred per year, with a mean of 18 failures per year.

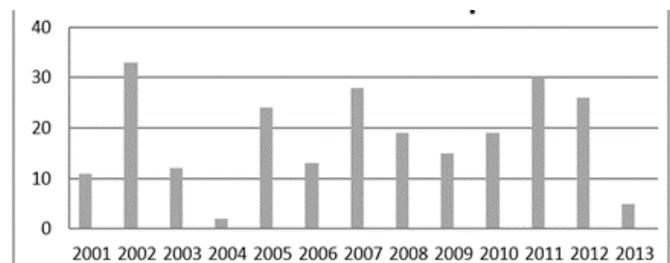


Figure 3. Number of failures per year.

All of the failure reports were carefully examined to diagnose the root cause of the failure. In order to ascertain trends and causes, the failures were sorted into the following categories: electrostatic discharge, electrical overstress, thermal overstress, mechanical overstress, foreign material, and chemical reaction.

Electrostatic discharge (ESD) is the failure mechanism that occurs when there is evidence on the semiconductor die of severe, localized damage. The indication is typically in the form of a crater or eruption through the insulating oxide layer seen only using extremely high magnification such as a scanning electron microscope.

Incidence of ESD damage involves almost instantaneous transfer of electrical energy coupled with a very high static potential. Thermal damage is minimal as compared to electrical overstress. Some reports mentioned instances in which device or circuit board handling was suspect with

respect to ESD control, but typically the damage induction is not recognized by the handler.

Electrical overstress (EOS) is a failure mechanism in which damage occurs to an electrical component that is operated above its absolute maximum electrical rated limits. EOS is similar to ESD, but typically is slower, and involves higher current, generating heat resulting in thermal damage. Often the failure involves other mechanisms such as conductive foreign material that creates a short circuit between two conductors resulting in excessive current. Another situation where EOS of a component can occur is during electrical testing using external power supplies.

Thermal overstress (TOS) is a failure mechanism in which damage occurs when the thermal energy exceeds the dissipation limits of a material. The source of the high thermal energy can be external such as from an oven or soldering iron or from an internal source such as excessive current during an EOS event. Additionally, the thermal energy also leads to material expansion, which can cause additional failure mechanisms. Once again, certain failure reports described scenarios that made the failure mechanism obvious such as the use of an improper temperature during thermal testing or exposure to excessive heat during soldering rework.

Mechanical overstress (MOS) is a failure mechanism in which damage occurs due to an excessive mechanical force. There were occasions when the damage was caused by external forces due to blatant operator error such as dropping a tool on a component or cracking a ceramic package due to excessive torque on a mounting bolt. Less obvious external forces caused cracking of glass seals around leads in ceramic packages, probably caused from improper component lead bend-and-trim operations. These mechanical forces can also be generated internally due to a thermally expanding encapsulant that provides a tensile force, causing a failure (e.g., lifting a gold wire ball bond off its pad).

Foreign material (FM), also referred to as foreign objects and debris (FOD), is defined as the presence of any material that is not designed into the product, or any material that is displaced from its original or intended position within the device. Tests used to detect the presence of foreign material include visual inspection, X-ray, particle impact noise detection, and energy-dispersive X-ray spectroscopy. Issues that can be caused by foreign material include poor adhesion of encapsulants, adhesives, solder and wire bonds (due to contamination between mating surfaces), and shorts caused by conductive particles between two conductors. Additionally, a source of foreign material can come from a loss of hermetic seal of a device allowing the entry of air and other contaminants (e.g., soldering flux) into its internal cavity.

Chemical reactions (CR) can be considered a subset of the foreign material category since usually there is foreign material present that acts as a reactant or catalyst.

Examples of chemical reactions include the formation of dendrites (which usually occurs in the presence of moisture) or the formation of intermetallic compounds between bonds of dissimilar metals.

Part of the analysis also included an attempt to deduce the time when the original defects occurred, which later resulted in a failure. An example scenario is a technician damaging a component via ESD during circuit board assembly, but the actual failure was not discovered until assembly level testing, much later in the development schedule. The failure report typically stated when the failure was discovered (e.g., during electrical or thermal cycling testing), but determining where the initial defect occurred was more challenging. For the purpose of this study, space system developers were referred to as component users, who procure components from the component manufacturers.

The goal of this portion of the analysis was to differentiate between defects induced by the manufacturers and ones induced by the users. The presence of foreign material or mechanical issues inside hermetically sealed devices were regarded as manufacturer-induced. Conversely, ESD defects were considered user-induced defects. Manufacturers typically have effective and regulated processes and techniques to prevent ESD damage to their specific parts. Conversely, defects caused by component installation onto printed circuit boards were considered user-induced.

There were 35 failures identified as ESD failures. The most common failure mechanism for microcircuits is ESD, while for passive components, the most common failure mechanism caused by human error was MOS.

B. Severity Factor for ESD

As previously noted, the risk of inducing a defect due to ESD is directly related to the sensitivity of the device to ESD damage. The ESD factor can be quantified with respect to an industry standard ESD rating for each component based on its sensitivity to damage. These standard ratings for ESD are shown in Table 1 [2, 3].

Electrical components are classified by their sensitivity to a high voltage electrostatic shock. The more sensitive the component, the lower the magnitude of voltage shock required to damage the component. Typically, ESD damage is induced with no warning or obvious signs on the component. While handling electronics, the generation of electric charge must be continuously monitored and mitigated.

Table 1. ESD rating and voltage thresholds.

ESD Rating	Voltage Threshold
0	< 250
1A	250 to < 499
1B	500 to < 999
1C	1,000 to <1,999
2	2,000 to < 3,999
3A	4,000 to < 7,999
3B	≥8,000

For background information, Table 2 shows typical electrostatic voltages that can be generated by human actions for two levels of relative humidity [4]. These values are extremely high, relative to the maximum ESD voltage ratings shown in Table 1. The reason that devices are not damaged more frequently is due to ESD-protected areas that have specific controls in order to prevent the generation of high electrostatic voltages. These areas use equipment and tools made of specific materials that prevent high electrostatic voltages from being generated. They also contain monitoring equipment that sounds an alarm if controls are not in a satisfactory condition [4].

Table 2. Typical electrostatic voltage generation values.

Means of Static Generation	Electrostatic Voltages	
	10–20% RH	65–90% RH
Walking across carpet	35,000	1,500
Walking over vinyl floor	12,000	250
Worker at bench	6,000	100
Vinyl envelopes for work instructions	7,000	600
Common poly bag picked up from bench	20,000	1,200
Work chair padded with polyurethane foam	18,000	1,500

C. Conclusions

This paper provides an introduction to ESD and the other common mechanisms that increase the risks of system failure due to human-induced defects in electrical parts. These risks extend from component manufacture to the integration and testing phases of system development, but more importantly, throughout mission life.

A risk analysis method is being developed that takes into account all these significant failure mechanisms and incorporates a unique severity factor for each of them. A significant benefit of this method is that it quickly communicates the greatest risk of potential electrical part failure due to human-induced defects in terms of part type and failure mechanism. This allows application of specific

mitigating actions to reduce the largest risks. If a risk assessment is conducted early in the design stage of system development, parts determined to have a high risk of becoming defective due to user error can be substituted for ones that have a lower risk. Similarly, processes can be altered making these user errors less frequent. The process becomes a “living” risk assessment, which is updated with respect to changes made to parts on the parts list and observing the effect that process changes have on the frequency of part failures.

As previously discussed, these failure mechanisms can cause defects in electrical components that do not always result in immediate failures; therefore, their condition may not be detected during testing. The environment in which electrical equipment will operate, such as space, adds significant but predictable stresses, such as vibration during liftoff and thermal cycling during transit. It is possible that electrical components, damaged during the assembly, integration and testing process, will fail when encountering these typical mission stresses, long before their predicted failure due to wear-out.

This article highlighted such risks of user-induced defects to sensitive components during system development and suggested specific areas to apply risk mitigation actions.

References

- [1] M. Tafazoli, “A Study of On-Orbit Spacecraft Failures,” *58th International Astronautical Congress*, Sept. 24-28, Sept. 2007, Hyderabad, India, pp. 6297–6308.
- [2] MIL-PRF-38535K, Paragraph A.3.4.1.4, *Integrated Circuits (Microcircuits) Manufacturing, General Specification for*, Defense Logistics Agency, Columbus, Ohio, Dec. 20, 2013.
- [3] MIL-PRF-38534K, Paragraph 3.9.5.8.2, *Hybrid Microcircuits, General Specification for*, Defense Logistics Agency, Columbus, Ohio, Nov. 15, 2017.
- [4] MIL-HDBK-263B, Appendix A, Table IV, *Electrostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Military Handbook*, Defense Logistics Agency, Columbus, Ohio Feb. 22, 1991.

For more information, contact:

Peter Majewicz 757-864-4474

Note: This article summarizes the ESD aspects of a longer and more comprehensive work yet to be released by Mr. Majewicz comparing various risks to electronic parts.

Contacts

NEPP <https://nepp.nasa.gov/>

Michael J. Sampson 301-614-6233
Michael.J.Sampson@nasa.gov

Jonathan Pellish
jonathan.pellish@nasa.gov

Peter Majewicz 757-864-4474
Peter.Majewicz@nasa.gov

NEPAG (within JPL)

<http://atpo.jpl.nasa.gov/nepag/index.html>

Shri Agarwal 818-354-5598
Shri.G.Agarwal@jpl.nasa.gov

Melissa Klose 818-354-4110
Melissa.Klose@jpl.nasa.gov

ATPO <http://atpo.jpl.nasa.gov>

Doug Sheldon 818-393-5113
Douglas.J.Sheldon@jpl.nasa.gov

JPL Electronic Parts <http://parts.jpl.nasa.gov>

Mohammad M. Mojarradi 818-354-0997
Mohammad.M.Mojarradi@jpl.nasa.gov

Jeremy L. Bonnell 818-354-2083
Jeremy.L.Bonnell@jpl.nasa.gov

Previous Issues:

Other NASA centers:

<http://nepp.nasa.gov/index.cfm/12753>

Public Link (best with Internet Explorer):

<https://trs.jpl.nasa.gov/discover?query=eee+parts+bulletin>

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

www.nasa.gov

National Aeronautics and Space Administration

Jet Propulsion Laboratory

California Institute of Technology
Pasadena, California

© 2019 California Institute of Technology.
Government sponsorship acknowledged.