National Aeronautics and Space Administration

EEE Parts Bulletin

Electrical, Electronic, and Electromechanical

A periodic newsletter of the NASA Electronic Parts Program / NASA EEE Parts Assurance Group and the Jet Propulsion Laboratory

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. 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. This third issue 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.

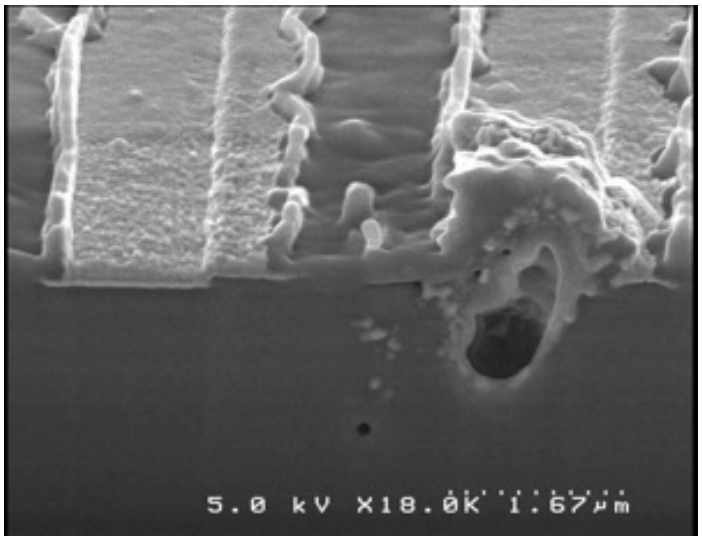

Figure 1. An ESD event of roughly 2.3 kV struck an RF transistor. The current caused a hole penetrating the underlying diffusions and an accumulation of material that re-solidified and shorted between the emitter and the collector (image courtesy of Hi-Rel Laboratories).

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.

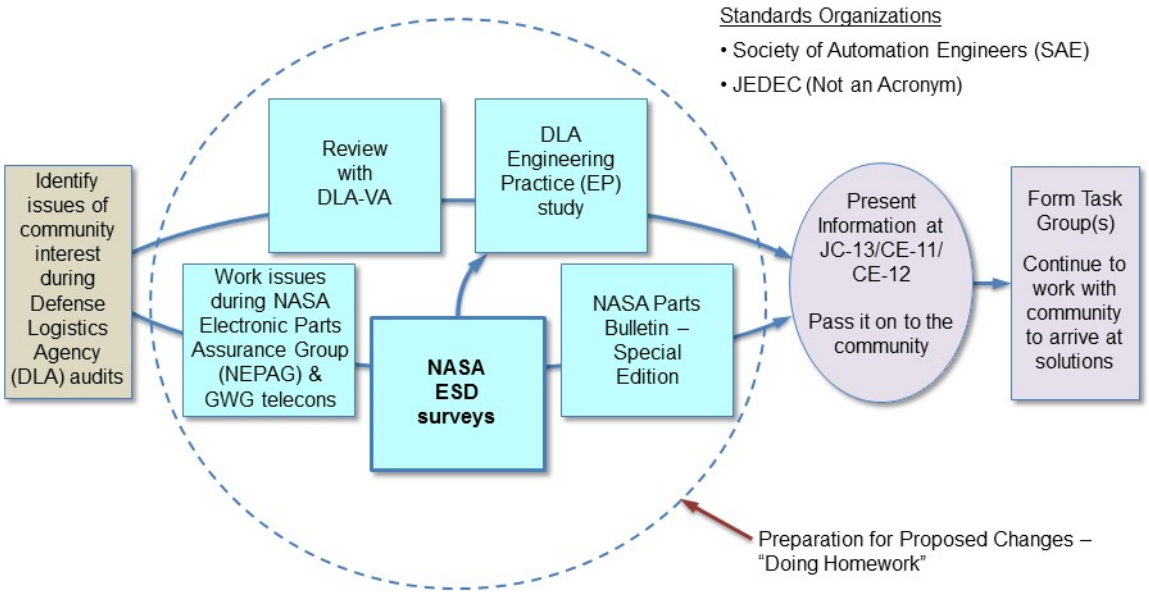

Figure 2. Changes to ESD standards as a sample of how observations from DLA audits and NASA ESD surveys raise issues and how resolutions are developed for those issues.

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)
- 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.
- 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 were 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 of 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.

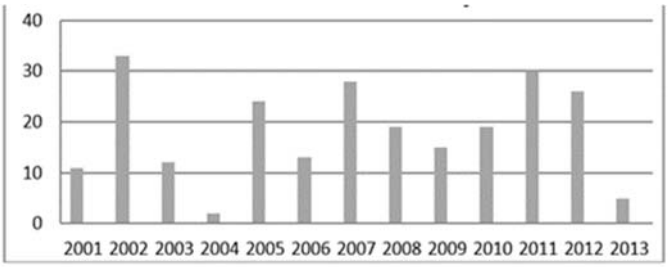

Figure. 3. Number of failures per year.

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 I. 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 alarms 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.

NASA Parts Specialists Recent Support for DLA Land and Maritime Audits performed at

- Aeroflex DBA Cobham, Colorado Springs, CO
- Aeroflex, DBA Cobham, Plainview, NY
- Amphenol Aerospace, Sidney, NY
- Amphenol Fiber Technologies, Allen, TX
- Amphenol-India, Pune, India
- Amphenol-India Mfg Services, Pune India
- Cirexx International, Santa Clara, CA
- DLA Precision Group, Holon, Israel
- E2v Aerospace & Defense, Inc., Milpitas, CA
- Henkel, Rancho Dominguez, CA
- Integra Technologies LLC, Wichita, KS
- International Rectifier, San Jose, CA
- IRC Incorporated, Corpus Cristi, TX
- Kyocera, San Diego, CA
- Microsemi Lawrence, Lawrence, MA
- Microsemi SoC Products Group, Mountain View, CA
- Micross Components, Orlando, FL
- Ohmite, Brownsville, TX
- Oneida Research Services, Englewood, CO
- Pacific Testing Lab, Valencia, CA
- Positronic, Pune, India
- Positronic Industries Inc., Mt. Vernon, MO
- Positronic Industries Inc., Springfield, MO
- Scientific Coatings, Santa Clara, CA
- Solitron Devices, Inc., West Palm Beach, FL
- SST Components Inc., Billerica, MA
- Teledyne, DBA e2v Aerospace & Defense, Grenoble, France
- Teledyne Microelectronic Tech, Lewisburg, TN
- Texas Instruments DMOS 5, Dallas, TX
- UHV Sputtering, Morgan Hill, CA
- Vishay Tansitor, Bennington, VT
- Vishay (Vitramon), Migdal Ham'emek, Israel

Upcoming Meetings

- JEDEC/JC-13 CE-11 & CE-12 meeting, Columbus, OH, Sept. 24–27, 2018

Contacts

NEPP https://nepp.nasa.gov/

Michael J. Sampson 301-614-6233
michael.j.sampson@nasa.gov

Kenneth A. LaBel 301-286-9936
kenneth.a.label@nasa.gov

NEPAG (within JPL)
http://atpo.jpl.nasa.gov/nepag/index.html
Shri Agarwal 818-354-5598
Shri.g.agarwal@jpl.nasa.gov

Roger Carlson 818-354-2295
Roger.v.carlson@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

www.nasa.gov
National Aeronautics and Space Administration

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California