A Risk Analysis Tool for Estimating the Risk of Electrical Failures Due to Human Induced Defects

Peter Majewicz, Ph.D.
NASA Langley Research Center

757-864-4474
peter.majewicz@nasa.gov

***Abstract*-Aerospace electrical systems are required to withstand and adequately operate in extremely harsh environments that include, for example, high radiation exposure, temperature extremes, intense vibrational stress and drastic temperature cycling. The nature of aerospace electronics also demands high reliability since, with very few exceptions, there is no chance for hardware servicing or repairs. Common risk mitigation techniques for this type of situation are to perform a Reliability Analysis of the system throughout the development cycle, and to use electrical components that are regarded as "high reliability" because of additional controls and requirements applied in their design, manufacturing and testing. Unfortunately, studies have shown that even though these techniques are used, many systems fail to meet mission requirements well before the predicted lifetimes.**

This paper presents the analysis of failures of electrical parts, experienced during various stages of system development, at NASA Goddard Space Flight Center, Greenbelt MD, between the years 2001 and 2013. These components were subjected to qualification, screening and testing in which the goal was to ensure that the components would survive the stresses of the mission. The analysis categorizes failures by part type and failure mechanisms.

One of the results of the analysis was the realization that a surprising proportion of failures experienced during system integration and testing were caused by human error (i.e. human induced defect). Further analysis included the determination of root failure mechanisms and any influencing factors contributing to these failures. The major causes of these defects were attributed to electrostatic damage (ESD), electrical overstress (EOS), mechanical overstress (MOS), and thermal overstress (TOS).

Finally, the study proposes a risk analysis tool which incorporates these major causes for the failures, termed error-producing conditions (EPCs), and a proportionality factor representing the number of each type of failure that has occurred at the facility under study. These factors are quantified and used to communicate the risk of human induced defects for the assembly, integration and testing of space hardware based on the system's electrical parts list. The new risk identification can trigger risk-mitigating actions more effectively, based on the presence of component categories or other hazardous conditions that have a history of failure due to human error.

The proposed methodology is demonstrated with an example.

TABLE OF CONTENTS

1. INTRODUCTION..... 2
2. RELIABILITY & HRA BACKGROUND..... 3
3. FAILURE REPORT ANALYSIS & RESULTS..... 4
4. INCORPORATION OF COMPONENT FAILURE DATA……..... 7
5. SUMMARY AND CONCLUSIONS.....10
APPENDIX….....11
ACKNOWLEDGEMENTS.....12
REFERENCES.....12
BIOGRAPHY 13

1. INTRODUCTION

Risk management is a vital project process whose purpose is to identify, analyze, treat and monitor risk continuously during the development of complex systems. The most basic and over-arching risk is one that describes system failure. Tracking the risk of failure is especially vital for electronic hardware destined for missions in outer space, since, with few exceptions, there is no chance for conducting repairs of the space system once it is deployed. Additionally, the cost associated with space systems makes the complete replacement of a malfunctioning satellite or planetary rover impractical. For these reasons, accurately identifying, analyzing and monitoring the risk of system failure is critical in order to assist everyone from design engineers to program managers with developing a system that will fulfill, and preferably surpass mission requirements.

There are unique challenges that make accurately calculating the reliability of electrical space systems (and conversely, the risk of failure) difficult. In general, the most effective source of data is from systems that have actually failed during operation in the intended environment (i.e. field failures). This type of physical analysis is essentially nonexistent since space systems, as mentioned previously, are rarely retrievable to allow for a failure analysis. With the lack of useful empirical data, another option is to conduct tests in laboratories to accumulate operational and failure data on the devices used in space system designs. This testing poses another issue, since development agencies cannot afford to purchase extra devices and assemblies for stress testing in quantities that would be statistically significant from which accurate failure models and reliability predictions can be devised. Additionally, the replication of the mission environment and duration in order to test hardware poses its own unique challenges of feasibility.

A common method for calculating the reliability of electrical systems is to use statistics and probability methods that provide quantitative data with reliability indices from testing by experimentation and by simulations. Additionally, a physics of failure (PoF) approach has gained considerable use as it seeks to quantify component reliability by investigating and modeling the root cause processes of device failures based on operational parameters and stresses.[1,2] The main criticism regarding these reliability calculation methods is that the predicted failure rates are not accurate when compared to failure rates observed in the field. Several studies have been conducted that documented numerous failures very early in the systems' predicted mission life. One of the studies showed a failure rate indicative of systems experiencing failures early in their life cycle, due to defects designed into or manufactured into the device (commonly referred to as infant mortalities).[3] This is in contrast to mature systems, that have predicted failures caused by wear out, after all mission requirements have been met.[4]

A possible cause for this discrepancy is the fact that most of these reliability calculation methods do not take into account possible defects introduced into electronic systems during system assembly, integration and testing, such as defects caused by technicians handling the devices. Such risks could be handled separately with a Human Reliability Assessment (HRA), but these methods also have accuracy issues and criticisms such as being overly dependent on expert opinion and the uncertainty of data concerning different human factors.[5]

The primary purpose of this study is to propose a risk analysis technique where factors based on electrical component failure data are used in a proposed Risk Analysis Tool. This visual tool, similar to the popular Risk Matrix, displays the relative risk of failure for all the electrical components, based on the major causes of electrical failures and a proportionality factor representing the quanitity of each type of failure that has occurred.

The main data source of this study is an analysis conducted on failure reports of electrical components from NASA Goddard Space Flight Center (GSFC) Failure Analysis Lab. These reports provide very in-depth investigations of components that failed between the years 2001 and 2013. The failures occurred to components during the system development phase starting at the point a component was received from the manufacturer and ending with fully integrated system testing. The focus of this analysis was to determine the failures caused by defects induced by technicians and other personnel handing the electronics. Using the information contained in the reports, the types of components that failed during different stages of system integration were categorized, and the mechanisms that contributed to these failures were determined. There was also an attempt to deduce where/when the original defect occurred that eventually caused the failures. This data was also the primary data source used to develop a technique for incorporating electrical component failure data into the HRA technique, Human Error Assessment and Reduction Technique (HEART).[6] The modification factors developed in this technique are used in this study.

2. RELIABILITY & HRA BACKGROUND

2.1 Reliability Analysis

A study of over 4,000 spacecraft missions from 1980 to 2005 was conducted by Mak Tafazoli of the Canadian Space Agency to determine the quantities of failures and their contributing factors that occurred between 1980 and 2005.[7] In a span of 25 years, more than 4,000 spacecraft were launched with 156 on-orbit failures recorded. For the author's analysis, a failure was defined as an incident that would either prevent the spacecraft from fulfilling its primary mission objectives (loss of mission) or cause a portion of the mission objectives to be abandoned (mission degradation). One of the major conclusions of Tafazoli's analysis was that many of the failures occurred before accomplishing their mission, even though they used relatively modern technologies and conducted thorough testing. Specifically, 40% of all failures happened within the first year of on-orbit activities, implying insufficient testing and inadequate modeling of the spacecraft and its environment. [7] The study further reveals that electrical failures were responsible for 45% of the total failures. The Power, Command and Data Handling (C&DH), and Telemetry, Tracking & Command (TTC) subsystems, which are dominated by electrical components, contributed to 54% of all failures with almost 50% of them occurring in the first year. Another conclusion of the analysis is that only 17% of the failures were caused by interactions with the space environment, such as solar and magnetic storms and space debris and meteorites, with 83% related to internal issues which include human error and design flaws. [7]

Another study also collected failure data for 1584 Earth-orbiting satellites successfully launched between 1990 and 2008. The authors conducted a nonparametric analysis of satellite reliability and demonstrated that a Weibull distribution with a shape parameter of less than one (<1), properly captures the on-orbit failure behavior of satellites.[3,4] A Weibull shape parameter of less than one is indicative of a decreasing failure rate, commonly referred to as infant mortality, a situation where devices are dead on arrival or fail very quickly in operation due to defects designed into or manufactured into the device. This is in contrast to the notion that due to the use of high reliability components and extensive testing, a Weibull distribution with a shape parameter fixed at 1.7 should be used for satellite systems, indicating failures due to wear-out mechanisms. The existence of a decreasing failure rate has been shown in additional studies of empirical data.[8-9]

2.2 HRA Methods

An HRA is a vital component of the larger-scoping Probabilistic Safety Assessments (PSA) and Probabilistic Risk Assessments (PRA). The goal of a PSA and PRA is to quantify a system's total risk (in terms of probability and severity) and identify issues that can have the greatest effect on safety. The HRA's focus is to quantify the probability of human error (i.e. an operator or technician fails to perform a given task or operation under a given condition), and determine the impact these human errors have on safety. Most industrial processes involve a great deal of human-machine interactions such as assembly, inspection, maintenance, operation and monitoring. The occurrence of errors can also be affected by other organizational factors such as training, experience, and work procedures, and programmatic concerns such as mission requirements, budget and schedule.

Although many HRA techniques were first developed by the nuclear industry during the 1970s and 1980s, such as Technique for Human Error Rate Predication (THERP) and HEART, many other industries tailored and utilized these methods to provide more relevant predictions that take into account industry-unique factors. Examples include the Hazard and Operability Analysis (HAZOP) and Explosive Atmosphere (ATEX) methods used in the chemical industry, and Eurocontrol Safety Assessment Method (SAM) for air traffic control. Other industries that have developed custom HRA methods include railway transportation, medical and offshore oil installations.[11-13] These industry methods identify specific risk-influencing factors (RIFs) and processes to quantify and incorporate them into their HEP calculation.[11]

The methodology proposed in a previous study used electrical component failure data to determine part categories and situations where failures occur more frequently due to human error. [6] The generic human error probabilities used in the HEART method were scaled with respect to the presence of these component categories and situations based on all electrical failures encountered. These factors are then used to produce the effective HEP.

The standard HEART method consists of thirty-eight Error Producing Conditions (EPCs) that may affect the task reliability, each with a corresponding weight ranging from 3-17. The selection of applicable EPCs and their respective weights is determined by an analyst. NOTE: To maintain consistency, this weight range (3-17) was also used for incorporating electrical part failure EPCs. There is an additional multiplicative factor, the Assessed Proportion of Affect (Ap_i), for

each EPC, ranging from 0 to 1, also determined by an analyst. For consistency, the methodology proposed in the previous study maintains the same format for EPC (range 3-17) and Ap_i (range 0-1) [6]. A key difference between the method contained in the previous study is that it uses analyzed failure data to determine the EPC weights and factors instead of relying on expert analysis, as typically done in the customized methods of other industries.

3. FAILURE REPORT ANALYSIS & RESULTS

The data that was analyzed for this study originated in failure reports spanning a period of approximately thirteen years, from January 2001 through September 2013. These detailed 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 is included describing the situation that led to the failure; for example, the component failed a visual inspection or electrical testing. Occasionally detailed information regarding the assembly history was 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. improper solder joint that was no longer present after the component was removed) or a fault that was intermittent. Figure 1 shows the number of failures that occurred per year, with a mean of 18 failures per year.

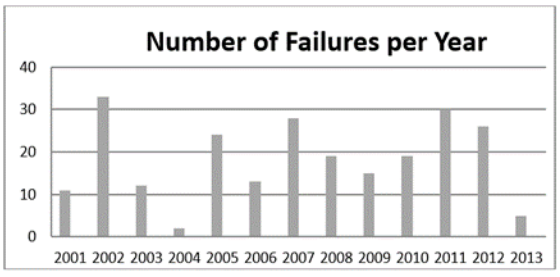

Fig 1 – Number of Failures per Year.

3.1 Failure Data Analysis

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, chemical reaction.

Electrostatic Discharge (ESD) is the failure mechanism that occurred when there was 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. The incidence of ESD damage involves an almost instantaneous transfer of electrical energy coupled with a very high static potential. Thermal damage is minimal as compared to Electrical Overstress. Some of the reports mentioned situations where the 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, 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 where 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 will also lead 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 where 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) is the category that 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 in a chemical reaction. 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.

The following figure depicts the quantities of failures as a function of failure modes.

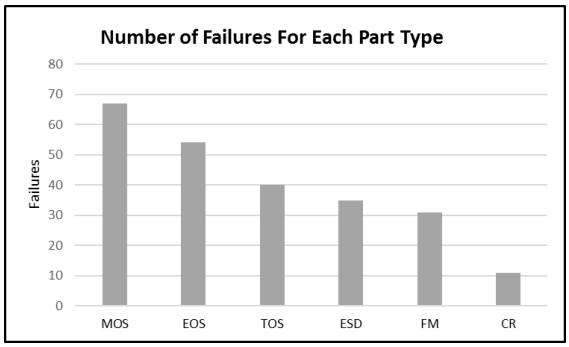

Fig 2 – Number of Failures of Each Part Type

3.1.1. Determining Defect Occurrence

Part of the analysis also included an attempt to deduce the point in 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 that were 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.

The number of failures that were induced by the users was more significant than expected. As discussed previously, information contained in various reports described situations such as improper trimming and bending of part leads damaging the glass seals around these leads, solder rework causing thermal stresses that induce micro-cracks in ceramic surface mounted components, and improper application of staking material which caused failures during vibration testing. Figure 3 shows that 41% of the failures were attributed to users. Figure 4 shows a breakdown of user-induced defects by part type. Figure 5 shows the total number of user-induced failures experienced due to the top three failure mechanisms.

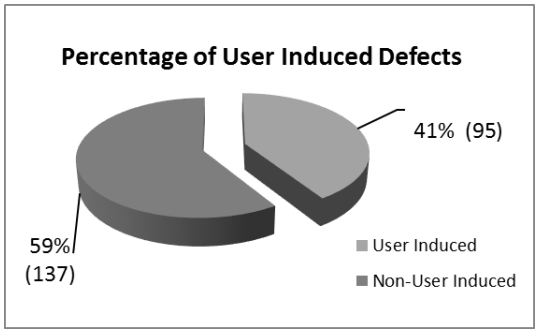

Fig 3 – Percentage of User-Induces Defects

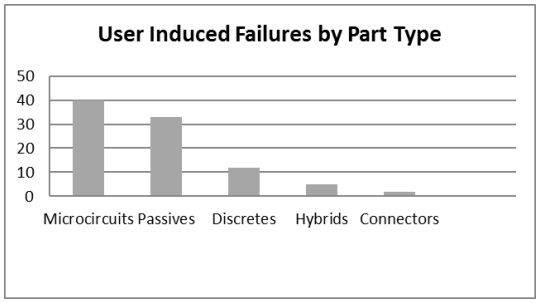

Fig 4 – User-Induced Defects by Part Type

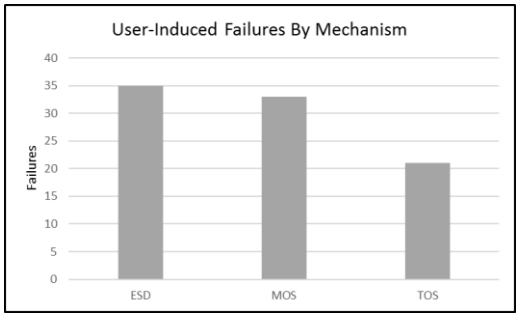

Fig 5 – Total User-Induced Defects by Mechanism

3.1.2. Concerns over User Induced Defects

The fact that so many defects were induced during component handling, system assembly, integration and testing is concerning for several reasons. First, some of the generated defects may cause immediate component failures. These failures should then be discovered during system testing, but the resulting is a program schedule delay as the failure is investigated, failure mechanism and collateral damage determined and finally the failed component replaced. In addition to the schedule penalty, there is also a budgetary penalty as additional resources need to be used to complete required actions (e.g. repairs, failure analysis). Secondly, these defects can cause latent failures that might not manifest until after mission commencement, when additional stresses are applied to the system (e.g. launch, thermal). The defects that were originally induced, such as micro-cracks in ceramic surface mount devices, may not grow large enough to cause a failure during burn-in or system testing, but may further propagate during the mission until a failure occurs. ESD damage is also a known risk for latent defects.[14-17] The final reason for concern is that the original reliability calculations for these designs typically do not take these user-induced defects and failures into account. A reliability calculation is typically conducted based on a list of parts in the circuit and a manufacturer provided failure rate for each component. Suppose a situation where two identical electronic circuit boards are being assembled at different facilities. A reliability assessment calculated based on the number of parts or on the physics of failure would be identical. However, if one facility used proper techniques, processes and equipment while the other had a history of inducing defects, the field reliability could be very different for each circuit board. This difference needs to be accounted for by having this risk of failure identified and tracked appropriately.

Figures 6 shows the breakdown of different failure mechanisms for microcircuits and passive devices, the two part types that experienced the most user-induced defects. The most common failure mechanism for microcircuits is ESD, while for passive components, the most common failure mechanism caused by human error was MOS.

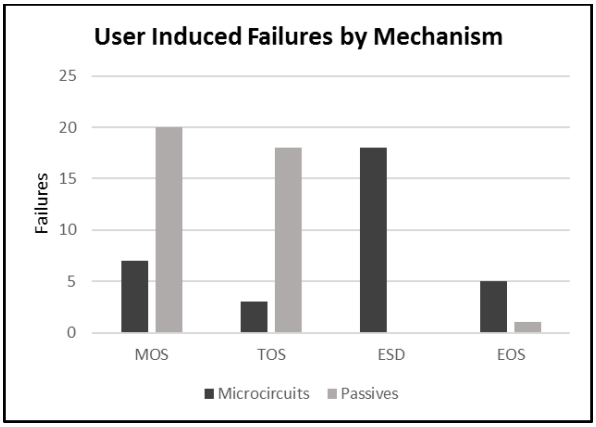

Fig 6 – User Induced Failures by Mechanism & Part Type

Figures 7 show the breakdown of each of the failure modes with respect to part types.

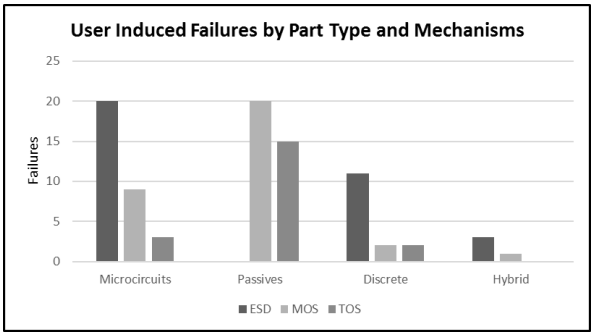

Fig 7 – User Induced Failures by Part Type & Mechanism

The remainder of this paper will expand on and demonstrate the proposed risk analysis methodology

that incorporates component failure data. Specifically, the data depicted in figures 6 and 7 will be used to quantify the risk for each failure mechanisms, while the Engineer's Assessed Proportion (Ap_i) will be calculated from the data depicted in figure 5.

4. INCORPORATION OF COMPONENT FAILURE DATA

Based on the information obtained from the failure analysis reports, the major failure mechanisms caused by user-induced defects were ESD overstress, mechanical overstress, and thermal overstress. These will be treated as Error Producing Conditions. The Engineer's Assessed Proportion (Ap_i) will be determined from the percentages of failures for each failure mechanism with respect to the total number of failures tracked (all failure mechanisms combined).This is consistent with the focus of HEART, in which the Engineer's Assessed Proportion signifies the degree of effect of each of the EPCs[10]. With the proposed method, the EPC is a measure of the sensitivity or vulnerability each of the individual electrical parts has to the different failure mechanisms, and the Ap_i is a function of the percentage of failed parts caused by the specific failure mechanism (EPC) to the total number of failed parts. For example, if a part is highly sensitive to a specific failure mechanism, the EPC will be a high value, potentially approaching the maximum EPC value of 17. Conversely, if the facility handling the part is specially equipped to handle the part without inducing defects caused by the same failure mechanism, the degree of effect ($i.e. Ap_i$) will reduce the contribution of that EPC. Finally, if a facility initially has numerous failures due to a specific failure mechanism, and then makes changes in order to lower the risk of inducing those defects, the respective Ap_i will be reduced as the number of failures goes down.

4.1. Individual Factor Calculation

As previously mentioned, 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 which is based on its sensitivity to damage. These standard ratings for ESD are shown in Table I.[18].

Table I. ESD Rating and Voltage Thresholds

ESD Rating	Voltage Threshold
0A	< 125
0B	125 to < 250
1A	250 to < 500
1B	500 to < 1000
1C	1000 to < 2000
2	2000 to < 4000
3A	4000 to < 8000
3B	>= 8000

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. For background information, Table II shows typical electrostatic voltages that can be generated by human actions for two different levels of relative humidity [37]. 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 [19].

Table II. Typical Electrostatic Voltage Generation Values

Means of Generation	10-25% RH	40 % RH
Walking across carpet	35,000V	15,000V
Walking across vinyl tile	12,000V	5,000V
Motion of Individuals Not Grounded	6,000V	800V
Remove Bubble Pack from Package	26,000V	20,000V
Poly bag picked up from bench	20,000V	10,000V

Table III shows the mapping of ESD ratings to EPC values. The EPC values range from 3 to 17 [10]. As mentioned earlier, this range is used in order to

maintain consistency with the original HEART method. The first column lists out all of the ESD ratings for electrical parts. The second column shows the respective EPC value. The values are a linear distribution with the most sensitive part rating, 0A, receiving the maximum EPC value of 17, and the least sensitive part, 3B, correlating to the lowest EPC value, 3.The values are reduced by 2 for each part category, as the sensitivity, and therefore risk, is reduced.

Table III. Mapping of ESD Categories to EPCESD Values

ESD Categories	EPC Value
0A	17
0B	15
1A	13
1B	11
1C	9
2	7
3A	5
3B	3

The Engineer's Assessed Proportion of Effect for ESD is the proportion of failures induced by the user caused by ESD to the total number of failures induced by the users, as shown in Equation 1.

$$Ap_{ESD} = \frac{n_{ESD}}{N} \quad (1)$$

where Ap_{ESD} represents the Engineer's Assessed Proportion of Effect for ESD, n_{ESD} is the total number of components that failed due to ESD and *N* represents the total number of failed components in the analyzed source data. As previously stated, this signifies the *degree of effect* of the EPC. It represents the probability that a failure was caused by the failure mechanism represented by the EPC out of all electrical failures. The use of empirical data to determine this proportionality effect is a major difference to methods that use expert judgment.

The EPC for mechanical overstress (EPC_{MOS}) can be quantified based on specific issues relating to part handling and the assembly process. One leading cause of failure due to MOS is a result of bending and cutting the leads of certain electrical components. This process is necessary in order for the component to be correctly mounted on the printed circuit board with all of the correct electrical connections. Since components come in various shapes, sizes and lead configurations, this process needs to be tailored for different parts. If the process is done incorrectly, the glass seal that surrounds each of the metal lead as it leaves the component body can be damaged, or possibly the component body itself may be damaged as indicated by cracks and chip-outs. Human error-induced defects can also be attributed to the improper handling of electrical components made from brittle materials such as ceramic, also indicated by cracks and chip-outs. These cracks may start out as micro-cracks, which may not be detected during inspection, but propagate and expand over time. Additionally, the improper staking of larger components can cause a part to fail during or after vibration testing. Each of these examples was observed in the source failure data.

The EPC_{MOS} is obtained from a careful analysis of the parts involved in the electrical hardware assembly being assessed for the likelihood of human error. The assessor will need information from the design and component engineers regarding the number of parts that require lead bend-and-trim operations or unique mounting techniques and the stresses encountered during these processes. Based on this information the assessor will assign each part a score between the values 0.18 and 1. An electrical part encountering more mechanical stresses during the assembly process will receive a score closer to 1. This score is then multiplied by 17 to generate the part's EPC_{MOS}. The resulting part's EPC weighting will be within the range of 3-17, consistent with the range of all other EPC's. The EPC_{MOS} for the assembly is obtained in the same way as with ESD, which is to calculate the mean of the individual parts' EPC_{MOS}. The Engineer's Assessed Proportion of Effect for MOS (Ap_{MOS}) is the proportion of failures induced by the user caused by MOS to the total number of failures induced by the users, obtained from the original failure data.

The EPC for thermal overstress (EPC_{TOS}) is obtained from a similar analysis of the parts involved in the electrical hardware assembly task. A significant number of parts from the source failure data analysis showed a detrimental contribution from touch-up soldering, a technique where a technician creates an initial solder joint which may not be satisfactory, and then reapplies the soldering iron to the component joint in order to redress it. Depending on the duration of time the soldering iron is applied, subsequently reapplied and the time in between, large temperature excursions may occur that cause irregular material expansion resulting in tensile stresses. These stresses can cause fractures in the material. Failed solder joints and thermal damage were also observed after repeated

soldering evolutions that were required to replace a failed component. Once again, the assessor will need information from the design and component engineers regarding the assembly process, specifically the soldering or epoxy techniques that will be used to mount the components. As with EPC_{MOS}, this information will then be used to generate a score between 0.18 and 1. This score will then be multiplied by 17 to obtain a EPC_{TOS} within the range of 3-17. The EPC_{TOS} for the assembly is obtained in the same way as with ESD, which is to calculate the mean of the individual parts' EPC_{TOS}. The Engineer's Assessed Proportion of Effect for MOS (Ap_{TOS}) is the proportion of failures induced by the user caused by TOS to the total number of failures induced by the users, obtained from the original failure data.

4.2 Risk Communication

As discussed previously, the goal of the proposed method is to provide system engineers and risk analysts a quantitative tool to manage and a visual tool to communicate the risk of electrical part failure caused by defects induced by users during system assembly, integration, and testing. A common way of communicating risk to multiple stakeholders is using a risk matrix, as it can streamline all risks into one picture and show relative rankings.[20] The proposed method utilizes a modified risk matrix (unidimensional risk factor vector (RFV)) to communicate the risk associated with electrical parts that are under analysis. Instead of the conventional axes representing "Probability" and "Consequence", only a risk factor (RF) associated with probability is represented and plotted on the horizontal axis. The RF is calculated for each part as the product of the EPCs for each of the failure mechanisms analyzed, and the Engineer's Assessed Proportion of Effect for each failure mechanism, respectively, shown in Equation 2, (shown for the ESD failure mechanism)

$$Risk\ Factor(i)_{ESD} = \frac{EPC_{ESD(i)} * Ap_{ESD}}{17} \qquad (2)$$

where i represents each individual electrical component in the assembly, $Risk\ Factor(i)_{ESD}$ represents the RF related to ESD for the ith component, $EPC_{ESD(i)}$ represents the EPC for ESD for the ith component, and Ap_{ESD} represents the Engineer's Assessed Proportion of Effect for ESD. The right-side product is divided by 17 since each of the failure mechanisms' EPCs was multiplied by a scaling factor of 17 in order to maintain consistency with the original HEART method. This scaling factor is not necessary for the RFV, since the resulting RFs will be between the range of 0 and 1.

To account for "consequence", an analysis such as a Failure Modes and Effects Analysis (FMEA) can be used to determine the *criticality* of electrical components, that is, to differentiate between critical and non-critical items. NASA defines "critical" as a condition where failure can "potentially result in loss of life, serious personal injury, loss of mission, or loss of a significant mission resource".[21] This will effectively correlate with consequence. Thus, a separate RFV can be populated for critical and non –critical components. Figure 8 shows an example of an unpopulated RFV. The RF for each part relative to each failure mechanism is plotted along the horizontal axis.

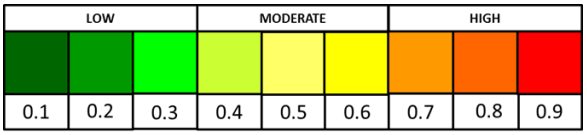

Fig 8 – Risk Factor Vector.

Several studies have been conducted that identified flaws in the use of risk matrices.[22-23] Most of the flaws stem from the fact that the matrix population requires quantitative determination of magnitude along two dimensions, in terms of consequence and probability. This process is usually accomplished by experts. The use of the RFV eliminates these flaws since (1) the source of plotted quantitative information is empirical failure data and (2) only a probability factor is plotted since the consequence is determined using an FMEA or similar tool.

4.3 Example Scenario

To illustrate the proposed method, an example will be used depicting a parts list for space flight electrical hardware. The generic part types and sensitivity factors are given in Appendix A.

The ESD, MOS and TOS ratings are shown for the parts in individual charts. The EPC magnitudes are obtained using the mapping of Table III for ESD, or from a simulated analysis of the mechanical and thermal stresses that the individual parts will see during assembly onto printed circuit boards and throughout system integration and testing. The Risk Factor Vector for the individual parts, with respect to failure mechanisms is shown in Figure 12. For clarity, only parts with a RF greater than or equal to 0.1 are shown. Additionally, if parts had the same RF value, the symbols were stacked vertically to remain legible.

The figure shows that the most risk lies in parts W (for MOS) and T, L, and J (for ESD). The original data for populating the RFV is shown in Table IV.

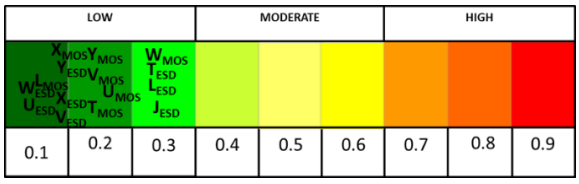

Fig 12 - Risk Factor Vector for Proposed Method Example

Table IV: Risk Factor Vector Data Table

ESD			MOS	
Part	**Risk Factor**		**Part**	**Risk Factor**
J	0.30		L	0.12
L	0.30		T	0.20
T	0.30		U	0.25
U	0.10		V	0.20
V	0.15		W	0.30
W	0.10		X	0.15
X	0.15		Y	0.20
Y	0.15			

Based on the Risk Factor Vector shown in Figure 5-2, Parts J, L & T show the highest risk of become defective due to human error due to ESD, and part W has the greatest risk of defect caused by MOS. The most effective course of action to reduce the probability of a part failure would be to verify the condition of all ESD handling equipment and review prevention procedures. Additional actions would be to review lead bend-and-trim operations, and a recommendation to practice on spare components. Additionally, if the Risk Assessment is made early enough in the design phase, a part with a high sensitivity to a failure mechanism may be substituted for one with lower sensitivity.

5. SUMMARY AND CONCLUSIONS

This paper proposes a methodology for incorporating electrical component failure data into program's Risk Assessment to more accurately assess and graphically communicate the risk of system failure due to human induced defects into electrical parts. This risk exists not only during the assembly, integration and testing phases of system development, but more importantly, during mission life. A parts list is used to demonstrate the method. The resulting Risk Factor Vector ranks the parts with the associated failure mechanisms in a color-coded format for easy communication. If the components used in the equipment were less sensitive, encountered less stress during the assembly process, or if their failures occurred less frequently in the past, then the expected Risk Factor would approach 0.

A significant benefit of this method is to quickly communicate the biggest risk of potential electrical part failure due to human-induced defects in terms of part type and failure mechanism. This allows specific mitigating actions to be taken to reduce the largest risks. If the Risk Assessment is conducted early in the design stage of system development, high risk parts can possibly be substituted for ones that have a lower probability of becoming defective due to user error. 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 will not result in immediate failures and therefore their condition may not be detected during testing. The environment in which electrical equipment will operate, such as outer space, adds significant, but predictable stresses, such as vibration during liftoff or 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. The goal of this proposed method is to highlight this risk of user-induced defects to sensitive components during system development and providing specific areas to apply risk mitigation actions.

Instead of using a risk matrix, the method utilizes a unidimensional risk factor vector to plot the risk of failure for each of the electrical parts relative to the failure mechanism for which it is most sensitive. The "consequence" component of a typical risk matrix is accounted for by dividing the components into critical and non-critical categories using an FMEA. Thus, a separate RFV can be populated for critical and non-critical components.

Appendix

Listing of parts, ESD rating, EPCs for ESD, MOS and TOS, and RFs for each individual part**.**

	Part Name	ESD Rating	EPC_{ESD}	EPC_{ESD}	EPC/17	RF = (EPC*Ap)/17	RF > 0.1
A	.22UF Capacitor	3B	3	3	0.176470588	0.063529412	
B	.68UF Capacitor	3B	3	3	0.176470588	0.063529412	
C	100nF Capacitor	3B	3	3	0.176470588	0.063529412	
D	100nF Capacitor	3B	3	3	0.176470588	0.063529412	
E	100pF Capacitor	3B	3	3	0.176470588	0.063529412	
F	200pF Capacitor	3B	3	3	0.176470588	0.063529412	
G	22nF Capacitor	3B	3	3	0.176470588	0.063529412	
H	Solid Tantalum Capacitor	3B	3	3	0.176470588	0.063529412	
I	Solid Tantalum Capacitor	3B	3	3	0.176470588	0.063529412	
J	1A Switching Diode	1A	13	13	0.764705882	0.275294118	0.28
K	1/8A Solid Body Fuse	3B	3	3	0.176470588	0.063529412	
L	P-Channel Mosfet	1A	13	13	0.764705882	0.275294118	0.28
M	5.11k Resistor	3B	3	3	0.176470588	0.063529412	
N	15.0k Resistor	3B	3	3	0.176470588	0.063529412	
O	5.62k Resistor	3B	3	3	0.176470588	0.063529412	
P	47 Resistor	3B	3	3	0.176470588	0.063529412	
Q	100k Resistor	3B	3	3	0.176470588	0.063529412	
R	10.0M Resistor	3B	3	3	0.176470588	0.063529412	
S	402k Resistor	3B	3	3	0.176470588	0.063529412	
T	MICROCIRCUIT, HYBRID, LINEAR, SINGLE DC DC Conv	1A	13	13	0.764705882	0.275294118	0.28
U	Precision Rail-to-Rail I/O Op Amp	3A	5	5	0.294117647	0.105882353	0.11
V	Precision Micropower Shunt Voltage Reference	2.00	7	7	0.411764706	0.148235294	0.14
W	12-Bit A/D Converter	3A	5	5	0.294117647	0.105882353	0.11
X	Crystal Oscillator Clock	2.00	7	7	0.411764706	0.148235294	0.15
Y	adjustable 3-terminal positive voltage regulators	2.00	7	7	0.411764706	0.148235294	0.15

	Part Name	MOS Factor	EPC_{MOS} = MOS Factor x 17	EPC_{MOS}	EPC/17	RF = (EPC*Ap)/17	RF > 0.1
A	.22UF Capacitor	0.15	2.55	2.55	0.15	0.051	
B	.68UF Capacitor	0.15	2.55	2.55	0.15	0.051	
C	100nF Capacitor	0.15	2.55	2.55	0.15	0.051	
D	100nF Capacitor	0.15	2.55	2.55	0.15	0.051	
E	100pF Capacitor	0.15	2.55	2.55	0.15	0.051	
F	200pF Capacitor	0.15	2.55	2.55	0.15	0.051	
G	22nF Capacitor	0.15	2.55	2.55	0.15	0.051	
H	Solid Tantalum Capacitor	0.20	3.4	3.4	0.2	0.068	
I	Solid Tantalum Capacitor	0.20	3.4	3.4	0.2	0.068	
J	1A Switching Diode	0.30	5.1	5.1	0.3	0.102	
K	1/8A Solid Body Fuse	0.20	3.4	3.4	0.2	0.068	
L	P-Channel Mosfet	0.35	5.95	5.95	0.35	0.119	0.12
M	5.11k Resistor	0.25	4.25	4.25	0.25	0.085	
N	15.0k Resistor	0.25	4.25	4.25	0.25	0.085	
O	5.62k Resistor	0.25	4.25	4.25	0.25	0.085	
P	47 Resistor	0.25	4.25	4.25	0.25	0.085	
Q	100k Resistor	0.25	4.25	4.25	0.25	0.085	
R	10.0M Resistor	0.25	4.25	4.25	0.25	0.085	
S	402k Resistor	0.25	4.25	4.25	0.25	0.085	
T	MICROCIRCUIT, HYBRID, LINEAR, SINGLE DC DC Conv	0.60	10.2	10.2	0.6	0.204	0.2
U	Precision Rail-to-Rail I/O Op Amp	0.70	11.9	11.9	0.7	0.238	0.24
V	Precision Micropower Shunt Voltage Reference	0.60	10.2	10.2	0.6	0.204	0.2
W	12-Bit A/D Converter	0.85	14.45	14.45	0.85	0.289	0.3
X	Crystal Oscillator Clock	0.40	6.8	6.8	0.4	0.136	0.14
Y	adjustable 3-terminal positive voltage regulators	0.55	9.35	9.35	0.55	0.187	0.19

	Name	TOS Factor	EPC_{TOS} = TOS Factor x 17	EPC_{TOS}	EPC/17	RF = (EPC*Ap)/17	RF > 0.1
A	.22UF Capacitor	0.40	6.8	6.8	0.4	0.088	
B	.68UF Capacitor	0.40	6.8	6.8	0.4	0.088	
C	100nF Capacitor	0.40	6.8	6.8	0.4	0.088	
D	100nF Capacitor	0.40	6.8	6.8	0.4	0.088	
E	100pF Capacitor	0.40	6.8	6.8	0.4	0.088	
F	200pF Capacitor	0.40	6.8	6.8	0.4	0.088	
G	22nF Capacitor	0.30	5.1	5.1	0.3	0.066	
H	Solid Tantalum Capacitor	0.20	3.4	3.4	0.2	0.044	
I	Solid Tantalum Capacitor	0.20	3.4	3.4	0.2	0.044	
J	1A Switching Diode	0.20	3.4	3.4	0.2	0.044	
K	1/8A Solid Body Fuse	0.20	3.4	3.4	0.2	0.044	
L	P-Channel Mosfet	0.30	5.1	5.1	0.3	0.066	
M	5.11k Resistor	0.40	6.8	6.8	0.4	0.088	
N	15.0k Resistor	0.40	6.8	6.8	0.4	0.088	
O	5.62k Resistor	0.40	6.8	6.8	0.4	0.088	
P	47 Resistor	0.40	6.8	6.8	0.4	0.088	
Q	100k Resistor	0.40	6.8	6.8	0.4	0.088	
R	10.0M Resistor	0.40	6.8	6.8	0.4	0.088	
S	402k Resistor	0.40	6.8	6.8	0.4	0.088	
T	MICROCIRCUIT, HYBRID, LINEAR, SINGLE DC DC Conv	0.30	5.1	5.1	0.3	0.066	
U	Precision Rail-to-Rail I/O Op Amp	0.25	4.25	4.25	0.25	0.055	
V	Precision Micropower Shunt Voltage Reference	0.20	3.4	3.4	0.2	0.044	
W	12-Bit A/D Converter	0.30	5.1	5.1	0.3	0.066	
X	Crystal Oscillator Clock	0.25	4.25	4.25	0.25	0.055	
Y	adjustable 3-terminal positive voltage regulators	0.20	3.4	3.4	0.2	0.044	

6. ACKNOWLEDGEMENTS

The author of this paper is grateful to his colleagues for their support, guidance and friendship, and to the team of technicians of the NASA Goddard Space Flight Center Failure Analysis Lab for their excellent work in relentlessly determining the failure modes of electronic devices.

REFERENCES

1. Snook I, Marshall J, Newman R. Physics of Failure as an Integrated Part of Design for Reliability. 2003 PROCEEDINGS Annual RELIABILITY AND MAINTAINABILITY Symposium. 2003 Jan 27-30; Tampa, FL. 46-54 p.

2. Varde P. Role of Statistical Vis-a-Vis Physics-of-Failure Methods in Reliability Engineering. Journal of Reliability and Statistical Studies. 2009; 2 (1): 41 – 51.

3. Castet J, Saleh J. Satellite and satellite subsystem reliability: Statistical data analysis and modeling. Reliability Engineering and System Safety. 2009; 94: 1718-1728.

4. Brown O, Long A, Shah N, Eremenko P. (2007), System lifecycle cost under uncertainty as a design metric encompassing the value of architectural flexibility. AIAA SPACE 2007 Conference and Exposition. 18-20 Sep 2007, Long Beach, California: 1-14 p.

5. Konstandinidou M, Nivolianitou Z, Kiranoudis C, Markatos N. Evaluation of significant transitions in the influencing factors of human reliability. Proceedings of the Institution of Mechanical Engineers Part EJournal of Process Mechanical Engineering. 2006; 222: 39-45.

6. Majewicz P., et. al. Estimating the Probability of Human Error by Incorporating Component Failure Data from User-Induced Defects in the Development of Complex Electrical Systems. Risk Analysis, an International Journal. 5 APR 2017, DOI: 10.1111/risa.12798

7. Tafazoli M. A Study of On-Orbit Spacecraft Failures. 58th International Astronautical Congress. 24-28 Sep 2007: Hyderabad, India. 6297-6308 p.

8. Krasich M. Reliability prediction using flight experience: Weibull adjusted probability of survival

method. NASA Technical Report, Jet Propulsion Laboratory, Document ID: 20060041898, April 1995.

9. Shooman L, Sforza P. A Reliability Driven mission for Space Station. Annual Reliability and Maintainability Symposium Proceedings. Seattle, Washington. 28 Jan 2002: 592-600 p.

10. Kirwan B. A Guide to Practical Human Reliability Assessment. Bristol, PA. Taylor and Francis; 1994.

11. Aven T, Hauge S, Sklet S, Vinnem J. Methodology for Incorporating Human and Organizational Factors in Risk Analysis for Offshore Installations. International Journal of Materials & Structural Reliability. Mar 2006; 4(1): 1-14.

12. Noroozi A, Khakzad N, Khan F, MacKinnon S, Abbasi R. The role of human error in risk analysis: Application to pre- and post-maintenance procedures of process facilities. Reliability Engineering and System Safety. 2013; 119: 251-258.

13. Lopez F, Bartolo C, Piazza T, Passannanti A, Gerlach J, Gridelli B, Triolo F. A Quality Risk Management Model Approach for Cell Therapy Manufacturing. Risk Analysis. 2010; 30(12) 1857-1871.

14. Reiner, Joachim C. Latent Gate Oxide Defects Caused by CDM-ESD. Electrical Overstress/Electrostatic Discharge Symposium Proceedings; 1995 Sep 12-14: 311-321.

15. Huh Y, Lee M, Lee J, Jung H, Li T, Song D, Lee Y, Hwang J, Sung Y, Kang S. A Study of ESD-Induced Latent Damage in CMOS Integrated Circuits. IEEE 36 Annual International Reliability Physics Symposium; 1998 Mar 31- Apr 2; Reno, Nevada: 279-283 p.

16. Greason W, Kucerovsky Z, Chum K. Experimental Determination of ESD Latent Phenomena in CMOS Integrated Circuits. IEEE Transactions on Industry Applications. July/August 1992; 28(4): 755-760.

17. Laasch I, Ritter H, Werner A. Latent Damage due to Multiple ESD Discharges. Electrical Overstress/Electrostatic Discharge Symposium Proceedings; 2009 Aug 30-Sep 4: Anaheim, CA, 308-313 p.

18. For Electrostatic Discharge Sensitivity Testing Human Body Model (HBM) – Component Testing. ANSI/ESDA/JEDEC JS-001-2014. Electrostatic Discharge Association and JEDEC Solid State Technology Association. 2014 Aug 28; p. 21 Table 3.

19. 3M. ESD control Handbook – Static Control Measures. [cited 2015 Sep 14] Available from: http://solutions.3m.com/3MContentRetrievalAPI/BlobServlet?locale=en_US&lmd=1154017253000&assetId=1114279231283&assetType=MMM_Image&blobAttribute=ImageFile

20. Elmonstri, M. (2014). Review of the Strengths and Weaknesses of Risk Matrices. Journal of Risk Analysis and Crisis Response, 4(1), 49-57.

21. NASA, (2013). Management of Government Quality Assurance Functions for NASA Contracts, NPR 8735.2. Revision Level B.

22. Cox, L. A. J., Babayev, D., & Huber, W. (2005). Some Limitations of Qualitative Risk Rating Systems. Risk Analysis, 25(3), 651-662.

23. Thomas, P., Bratvoid, R.B., Bickel, J.E., (2014). The Risk of Using Risk Matrices. April 2014 Society of Petroleum Engineers - Economics & Management. 56-66

BIOGRAPHY

Peter Majewicz *received a B.S. in Computer Engineering from Old Dominion University, Norfolk, CA, in 1999, a M.S. in Electrical Engineer from the Naval Postgraduate School in Monterey, CA in 2005 and a Ph.D. in Systems Engineering from George Washington University, Washington D.C. in 2017. He has been with NASA since 2009, working in the EEE Parts Office, Electronics Systems Branch, Engineering Directorate. Prior to NASA, he retired from active duty, ending a 22 year career in the U.S. Navy.*