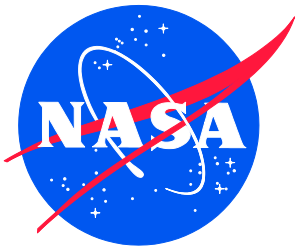
NASA/TM–2019-220269
NESC-RP-17-01211



Radiation Single Event Effects (SEE) Impact on Complex Avionics Architecture Reliability

Robert F. Hodson/NESC
Langley Research Center, Hampton, Virginia

Dwayne Morgan
Wallops Flight Facility, Wallops Island, Virginia

Raymond L. Ladbury
Goddard Space Flight Center, Greenbelt, Maryland

Yuan Chen
Langley Research Center, Hampton, Virginia

Michael Bay, and Jeffrey Zinchuk
Bay Engineering Innovations, Inc., Edgewater, Maryland

April 2019

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

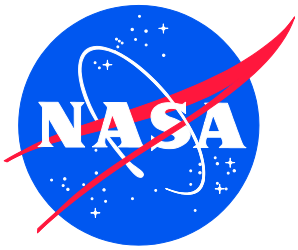
- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question to help@sti.nasa.gov

- Phone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM–2019-220269
NESC-RP-17-01211



Radiation Single Event Effects (SEE) Impact on Complex Avionics Architecture Reliability

Robert F. Hodson/NESC
Langley Research Center, Hampton, Virginia

Dwayne Morgan
Wallops Flight Facility, Wallops Island, Virginia

Raymond L. Ladbury
Goddard Space Flight Center, Greenbelt, Maryland

Yuan Chen
Langley Research Center, Hampton, Virginia

Michael Bay, and Jeffrey Zinchuk
Bay Engineering Innovations, Inc., Edgewater, Maryland

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

April 2019

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

NASA Engineering and Safety Center
Technical Assessment Report

Radiation Single Event Effects (SEE) Impact on Complex Avionics Architecture Reliability

March 21, 2019

Report Approval and Revision History

NOTE: This document was approved at the March 21, 2019, NRB. This document was submitted to the NESC Director on March 27, 2019, for configuration control.

Approved:	*Original Signature on File (MK)*	3/28/19
	NESC Director	Date

Version	Description of Revision	Office of Primary Responsibility	Effective Date
1.0	Initial Release	Dr. Robert F. Hodson, Technical Fellow for Avionics, LaRC	03/21/19

Table of Contents

Technical Assessment Report

List of Figures

List of Tables

Technical Assessment Report

1.0 Background

The NASA Engineering and Safety Center (NESC) has an urgent need to understand how system-level reliability of an avionics architecture is compromised when portions of the architecture are temporarily unavailable due to single event effects (SEE). The proposed activity parametrically evaluated these SEE impacts on system reliability based on mission duration, upset rate and recovery times for a representative redundant architecture.

The key stakeholders for this study are NASA programs and projects that expect to use avionics architectures with electrical, electronic and electromechanical (EEE) parts susceptible to SEE when exposed to the mission expected radiation environment.

2.0 Signature Page

Submitted by:

Team Signature Page on File – 4/9/19

Dr. Robert F. Hodson Date

Significant Contributors:

Mr. Dwayne R. Morgan Date

Dr. Raymond L. Ladbury Date

Dr. Yuan Chen Date

Mr. Michael Bay Date

Mr. Jeffrey Zinchuk Date

Signatories declare the findings, observations, and NESC recommendations compiled in the report are factually based from data extracted from program/project documents, contractor reports, and open literature, and/or generated from independently conducted tests, analysis, and inspections.

3.0 Team List

Name	Discipline	Organization
Core Team		
Robert Hodson	Lead, NASA Technical Fellow for Avionics	LaRC
Michael Bay	Avionics Technical Discipline Team (TDT)/ Systems Engineering TDT	GSFC, Bay Engineering Innovations
Yuan Chen	Avionics TDT	LaRC
Raymond Ladbury	Technical Lead, Avionics TDT	GSFC
Dwayne Morgan	Technical Lead, Avionics TDT	GSFC
Jeffrey Zinchuk	Avionics TDT/GN&C TDT	GSFC, Bay Engineering Innovations
Business Management		
Loutricia Johnson	MTSO Program Analyst	LaRC
Administrative Support		
Linda Burgess	Scheduler	LaRC/AMA
Melinda Meredith	Project Coordinator	LaRC/AMA
Erin Moran	Technical Editor	LaRC/AMA

4.0 Executive Summary

Whether in terms of size, weight, power, speed, precision or a range of other metrics, commercial state-of-the-art (SOTA) electrical, electronic, and electromechanical (EEE) parts are outperforming their space-qualified counterparts by increasing margins. More and more, these performance advantages are becoming crucial for space missions to achieve ambitious performance goals. However, most of these parts are designed for terrestrial applications, and their use in space environments often introduces susceptibilities to single event effects (SEE) that may pose significant threats to mission success.

Unless space mission design teams develop sufficient understanding of SEE susceptibilities and model their effects on a system, these fault and failure modes can overwhelm intended system-level reliability and safety, resulting in system failure.

SEEs can cause a broad range of anomalies and irrecoverable failures, including momentary disturbances of a part's output to data corruption, recoverable loss of functionality, or catastrophic failure. Resulting system-level consequences may depend on the operating state of the affected part, its application in the system, and even the system's state at the time of the SEE. This complex behavior has made it difficult to include SEE in most reliability estimates. However, the increasing use of SOTA and commercial-off-the-shelf (COTS) parts has made such inclusion increasingly important.

System-level modeling can explore system sensitivity to SEE rates and consequences when details of the performance of constituent parts remain uncertain, and can establish upper bounds on the SEE rates necessary for acceptable system performance. Such sensitivity modeling results can guide comprehensive SEE testing of critical parts driving system performance, reliability, and safety. This facilitates ensuring EEE component rates remain within acceptable bounds.

System-, element-, unit-, and component-level redundancy are approaches to mitigate SEE. Bounding the SEE threat is especially important when using system-level redundancy to mitigate errors and failures that are non-reparable at the element or individual unit level.

This NESC study focuses primarily on:

1) Developing methodologies for including non-reparable SEE rates and reparable SEE rates (with anticipated repair times) in system-level risk modeling to ensure that the radiation effects in electronics are not a significant mission risk contributor.
2) Applying the results of parametric system-level risk modeling to guide the SEE component test and analyses efforts to ensure the bounding limits used in the model are appropriate.

The NESC team developed guidelines for using system-level modeling to develop insights into system vulnerabilities before SEE becomes a significant threat to mission success, for identifying characteristics that may render a system particularly vulnerable to SEE, and for using results of system-level modeling to optimize testing, analysis, and verification efforts in terms of system-level risk reduction. These guidelines are summarized below.

Based on the studies done, the following guidelines were developed to ensure system modeling yields results that provide useful guidance for radiation and reliability analysis:

1) Irreparable and reparable SEE rates should be included in system models.

2) Reliability and availability model sensitivities should be investigated over a range of rates for reparable and irreparable events and recovery times to determine the level at which they significantly detract from mission success.
3) System-level models should be sufficiently complex to reflect impacts of operating through different mission phases and with different levels of resilience.
4) If system redundancy serves multiple purposes, all of these purposes must be included in the system models, along with their interferences with each other.

The following guidelines were developed to ensure that SEE testing and analysis efforts make efficient use of system modeling results:

1) Use results of system-level reliability and availability assessments to guide SEE test and analysis efforts.
2) Bound unit and system failure rates using available data to determine whether system SEE rates could affect failure rates unacceptably based on system modeling results.
3) Use testing and analysis approaches that are consistent with the program's risk position and risk factors
4) Prioritize testing based on system-level simulation results and risk, ranking, and expected benefits.
5) To minimize disruption to the design process, develop work-around or redesign strategies for use if one or more of the parts selected for test exhibit unacceptable SEE.

The guidelines noted above are discussed in more detail in Section 7.2.

5.0 SEE Threats and Use of Redundancy

System failures can occur due to a variety of causes (e.g., mechanical failures, thermal failures, electrical failures, wear-out). In most systems, non-electrical failures (e.g., parachutes, engines, structures, tanks) dominate the system failure causes since these failure rates are bounded by material capabilities and physics. Electrical and avionics components are usually highly reliable and not a significant contributor to mission failure (on the order of <1%). Additionally, electrical components' reliability can be supplemented via redundancy, making their contribution to the system failure rate minimal. Ensuring electronics risk does not drive mission risk by more than a few percent requires electronics failure rates to be orders of magnitude smaller than non-electrical failure rates.

Figure 1 illustrates how non-electrical failures with a system failure rate of 1 lost mission per 200 attempted missions (99.5% probability of mission success) combine with electrical failures of 1 loss per 20,000 attempts (99.995% probability of avionics success) to reduce the total mission failure rate (i.e., loss of mission (LOM)) to 1 in 198 (or a 99.495% probability of success)[1]. If the electrical failure contribution is 1% of the non-electrical failure, it will have a commensurate effect on the system failure rate.

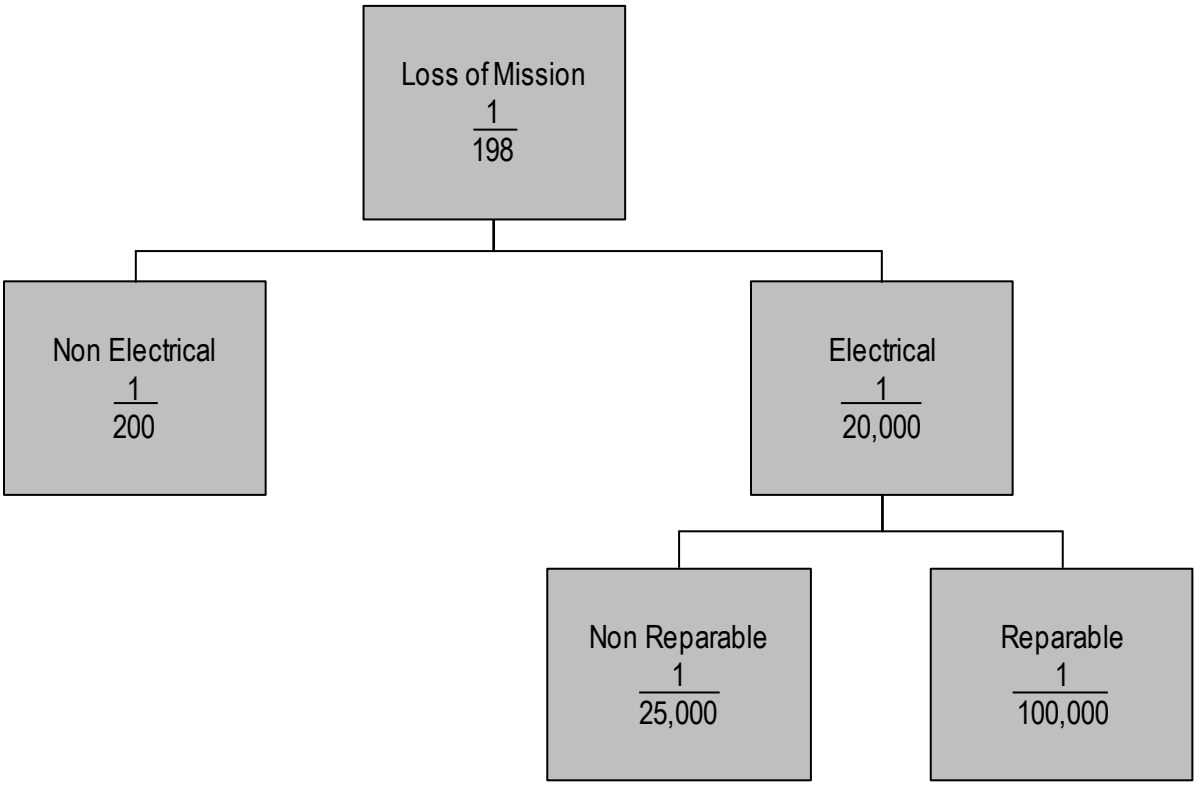


Figure 1. Notional Non-Electrical and Electrical Failure Rate Contributors to LOM

Figure 1 shows that electrical failures can be classified as reparable or non-reparable. Reparable failures include momentary disturbances, data corruption, or loss of functionality (i.e., nondestructive SEE (NDSEE)), and non-reparable failures are catastrophic (i.e., destructive

[1] Use of Commercial Electrical, Electronic, and Electromechanical (EEE) Parts in NASA's Commercial Crew and Cargo Program, TI-12-00762, 3/15/2012

SEE (DSEE)). This is especially important in a space environment, where nondestructive SEEs can temporarily result in a component failure, but not prohibit the component from recovering and continuing to perform its function after the repair time. Depending on the system application, these repairs can be automated and self-correcting or they may require an external command to initiate the repair cycle. In either case, the time to SEE repair and recovery must be considered in the reliability assessment model, especially when the recovery is not instantaneous. The recovery time from SEEs is application-dependent, and can vary from microseconds to minutes to hours.

Figure 2 shows the frequency of system failure as function of the electrical failure frequency (e.g., due to issues with packaging, wiring, workmanship), assuming a constant non-electrical failure rate of 1 per 200 mission attempts. As noted above, electrical failure probabilities are usually a small fraction of the dominant non-electrical failure probabilities. However, as discussed below, SEE-induced failures can cause failures due to electrical components to rival or even exceed the non-electrical failure rate.

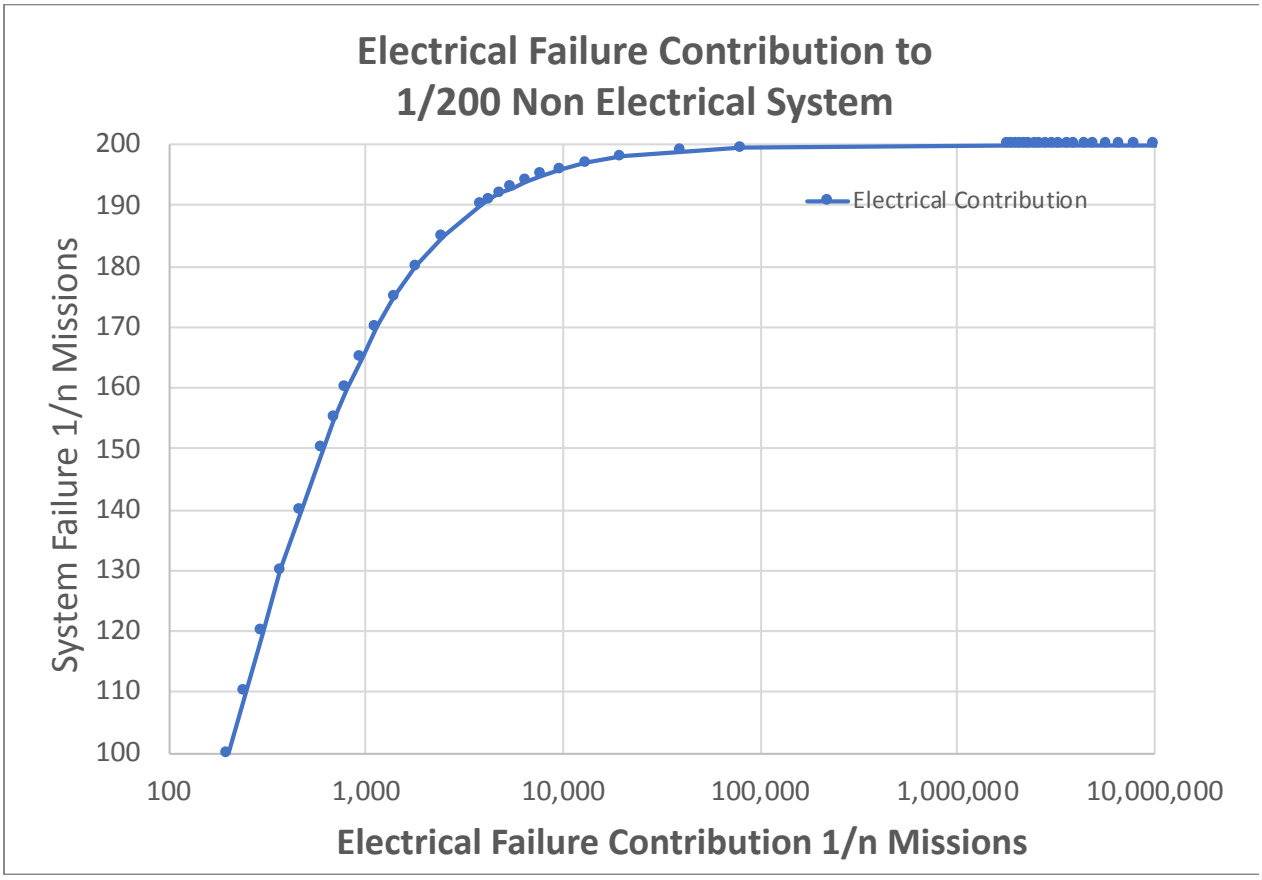


Figure 2. Electrical Failure Rate Contributors to LOM

5.1 SEE Threats

The space radiation environment poses threats to systems that have no analog in terrestrial applications. These threats include dose effects and SEE. Dose effects accumulate over the life of the mission, resulting in degraded performance and an increasing probability of failure as the mission progresses. Because failure rates due to dose effects increase over time, and because this cumulative degradation occurs for all parts (biased or not), redundancy is ineffective as a mitigation approach. Applications often require application of a design margin to the dose

capabilities of components to ensure this failure type is negligible. In contrast, SEEs occur with a constant failure rate (i.e., any two identical particles have the same probability of causing the effect). Since radiation environments are close to "average" conditions most of the time, SEEs are treated as constant failure-rate processes over much of the mission and are candidates for redundant mitigation strategies. In this study, the NESC team concentrated on SEEs and their effects on redundant systems.

SEEs occur when an ionizing particle traversing a region of the device sensitive to the effect (called the sensitive volume) deposits sufficient energy in that region to generate the effect. The part technology and application conditions determine which SEE modes are of potential concern for a given part. The consequences of the SEE at the system level are even more application-dependent, depending not just on device function, but also on the system's state when the SEE occurs. Figure 3 illustrates the main SEE modes and the technologies that may be susceptible to them.

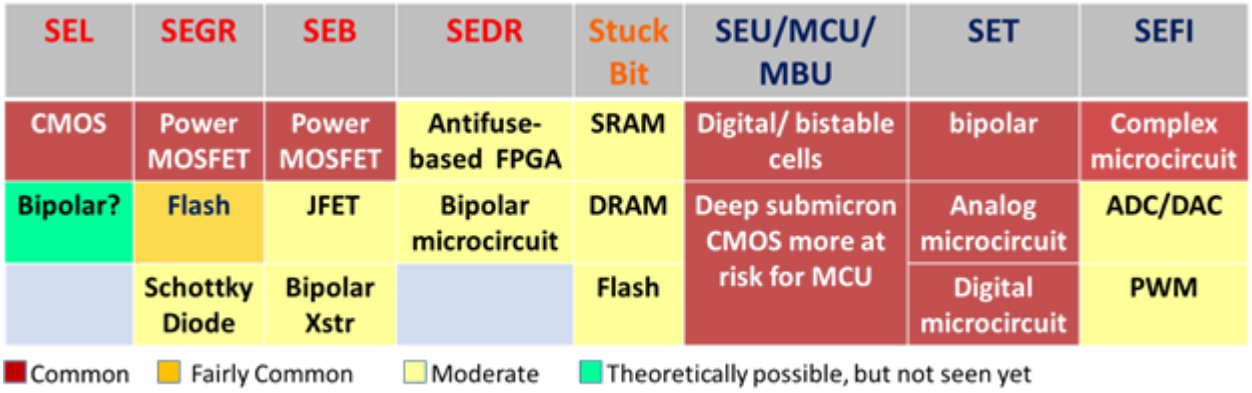


Figure 3. Main SEE Modes and Technologies that may be Susceptible

Destructive modes are indicated in red text in the top row, while nondestructive SEEs are indicated by blue text. Stuck bits represent a special case, since they affect only part of the device (e.g., one bit in a memory) and they repair themselves (a process called annealing) over time. For brief definitions of the types of SEE listed in the top row of the table, see Section 10.0, Definition of Terms.

The risk a SEE mode poses at the part level depends on the consequences of the mode (e.g., flipped bits, lost functionality, or failure) and the occurrence rate. Unfortunately, unless the parts used in the system are specifically intended for use in space or have a successful history in applicable heritage missions, these risk determinants may be unknown and must be determined through SEE testing and/or analysis. The standard method for revealing SEE susceptibilities and determining the corresponding rates is heavy-ion testing, which involves irradiating the part with high fluences of ions representative of the mission environment. Unfortunately, heavy-ion testing is costly, difficult, and time-consuming, especially for complex SOTA and COTS parts. This has led to development of alternative methods for identifying potential SEE risks and bounding SEE rates. These methods include:

1) Use of proton SEE data to bound heavy-ion risk for parts that are highly SEE sensitive.
2) Use of data for similar parts fabricated in the same process to identify potential SEE susceptibilities and bound their SEE rates.

3) Use of heritage data for the part in an equivalent or bounding space mission.

The first two methods can provide bounds to SEE modes, but they cannot reliably detect or bound susceptibilities to all modes, especially to DSEE [2] [3]. Use of heritage data requires a thorough understanding of the similarities and differences between the completed and proposed missions. In addition, as will be discussed, use of heritage data for systems using redundant mitigation for SEE poses specific challenges. Uncertainties in NDSEE, and especially DSEE rates as bounded by these alternative methods, make it difficult to ensure SEE rates remain sufficiently low that they do not overcome mitigation. Other issues that could make SEE mitigation challenging include:

1) SEE rates in space exceed terrestrial rates by many orders of magnitude. Moreover, the energetic and highly ionizing particles in the space environment can cause SEE modes that would never be seen in terrestrial applications. Unless the parts are intended and designed for space, the only way such threats will be revealed is through appropriate SEE characterization.
2) SEE behavior in some parts involves multiple SEE modes with different consequences, and these may require multiple and diverse redundancy schemes.
3) Although SEEs are Poisson processes, they are Poisson in particle flux rather than time, so their rates can vary throughout the spacecraft's orbit or over time due to solar activity. Particle flux is a key driver to the SEE rate.
4) Increasing use of COTS parts means that more parts selected for space systems have unknown SEE susceptibilities that must be revealed through expensive, technically demanding, and time-consuming test campaigns[4].
5) The increasing complexity of COTS parts has made it more tempting to employ alternate SEE test methods (e.g., board or box-level proton SEE testing). These alternate methods could reduce testing cost and duration, but at the expense of detailed understanding of the SEE susceptibilities.
6) Mitigation of SEE complicates system designs and may result in penalties to performance and/or size, weight, and power (SWAP) constraints on the system design.

5.2 Rationale for Redundancy

Component-, unit-, element-, and system-level redundancy implementations are important techniques for meeting system requirements for performance, availability, and reliability even when the individual components making up the system do not meet required reliability. Redundancy is used to meet different mission requirements, including operational lifetime, safety and fault tolerance, error detection, and SEE threats.

[2] R. Ladbury and M. Campola, "Bayesian methods for bounding single-event related risk in low-cost satellite missions," IEEE Trans. Nucl. Sci., vol. 60, no. 6, pp. 4464–4469, Dec. 2013.

[3] R. L. Ladbury and J.-M. Lauenstein, "Evaluating constraints on heavy-ion SEE susceptibility imposed by proton SEE testing and other mixed environments," IEEE Trans. Nucl. Sci., vol. 64, no. 1, pp. 301–308, Jan. 2017.

[4] Testing at the Speed of Light—The State of U.S. Electronic Parts Radiation Testing Infrastructure, Washington, D.C.: National Academy of Sciences, pp. 27-28 (2018).

For lifetime objectives, when a required unit fails, its operation could be replaced by a redundant component, allowing the function to continue and avoiding LOM. Redundancy is also implemented to satisfy safety-critical requirements for human-crewed missions. In some cases, even when the individual component or unit is highly reliable and each unit's expected lifetime exceeds the mission timeline, redundancy may be required to meet fault tolerance requirements, ensuring that an *unexpected* component anomaly does not jeopardize the mission.

Redundancy is employed to perform detection, localization, and reconfiguration for component failures. When a system must meet time-critical performance, redundancy can be used to instantly detect and identify the failed component. This is commonly used in computer applications with self-checking pairs (SCP), or it can be used as a three-for-one voting scheme. This redundancy for fault detection isolation and recovery (FDIR) can be applied at multiple levels (e.g., the component, subsystem, or system level).

Finally, redundancy is used to handle environmental effects, including temporary disruption of a function due to SEE, which is the focus of this study.

It is important to note that when a leg of redundancy is removed due to transient or permanent failure, the system will be operating in a degraded state. The loss of a single string due to SEE, even temporarily, will have an impact on system reliability, availability, and performance. If the SEE responses of the components in a system are poorly understood, then SEE fault rates may dwarf those due to other causes. This can be a significant concern. Conventional reliability calculations do not consider SEE-induced faults, because parts for space applications were selected for their SEE immunity. However, in a system where COTS parts are used, such immunity is not assured. Even if all SEE modes are recoverable, the design must account for the unavailability of the recovering element to serve as a redundant backup during recovery from an SEE.

5.2.1 Redundancy Implementation to Improve System Performance

To explore how the redundancy can be used to meet the mission lifetime requirements, assume that a critical system for a short mission (e.g., a 15-minute launch-vehicle mission) must achieve 99.5% reliability considering only electrical failures. If the system uses three units configured into redundant elements to meet its required performance, then the unit failure rate can be as high as 0.75 failure per hour. The second unit performs the function after the first unit fails, and the third unit completes the mission after the first *and* second units have failed. Therefore, the mission reliability expectation can be met by using redundant elements to replace the failed components. It would take three concurrent or overlapping component failures to compromise mission reliability.

5.2.2 Redundancy Implementation for Safety-critical Functions

Redundancy also enables system performance to address unanticipated failures or errors of components required in critical functions. Even when individual parts are expected to last the entire mission, redundancy is designed into the system to address unknown and unanticipated loss of components due to external events. Many of NASA's human-rated systems for launch

vehicles,[5] International Space Station (ISS) visiting vehicles,[6] and inhabited orbiting platforms (e.g., Deep-Space Gateway, commercial platforms) have requirements for specific levels of fault tolerance. These redundant implementations are irrespective of the implementation to address reliability, performance, and known environmental conditions

5.2.3 Redundancy Implementation for FDIR

Redundancy is used for the FDIR function coverage. If triple redundancy is employed and all three elements are available and operational, then their outputs can be voted to correct errors that occur within any single unit. This implementation may be used to replace internal types of FDIR (e.g., rate or range limits, model comparison) the units would need to employ if the redundant components were not available for direct comparison. Many complex systems have used redundant implementations to simplify the internal built-in test and FDIR software development, test, and qualification typically used to detect circuit faults and errors. With a voting or comparison strategy, detecting a circuit or component experiencing an anomaly is straightforward. When all three units are available (3:3), the system can detect the faulty string and continue seamless operation with the remaining healthy strings. If only two of the three units are available (2:3), the outputs can be compared to detect discrepancies and prevent propagation of an error (e.g., by entering a safe state and requesting intervention or by retrying the calculation).

Figure 4 illustrates a system where non-electrical causes contribute 1 mission failure every 200 missions in series with an electrical element consisting of three units. Only when all three units fail does the element (and therefore the mission) fail. The element is considered 3-for-1 or 3:1 redundant, since the survival of any of the three redundant units constitutes mission success.

[5] ISS Crew Transportation and Services Requirements Document, CCT-REQ-1130 Rev D-1, 3-23-2015

[6] International Space Station (ISS) to Commercial Orbital Transportation Services (COTS) Interface Requirements Document (IRD), SSP-50808 Rev F, 9-2014

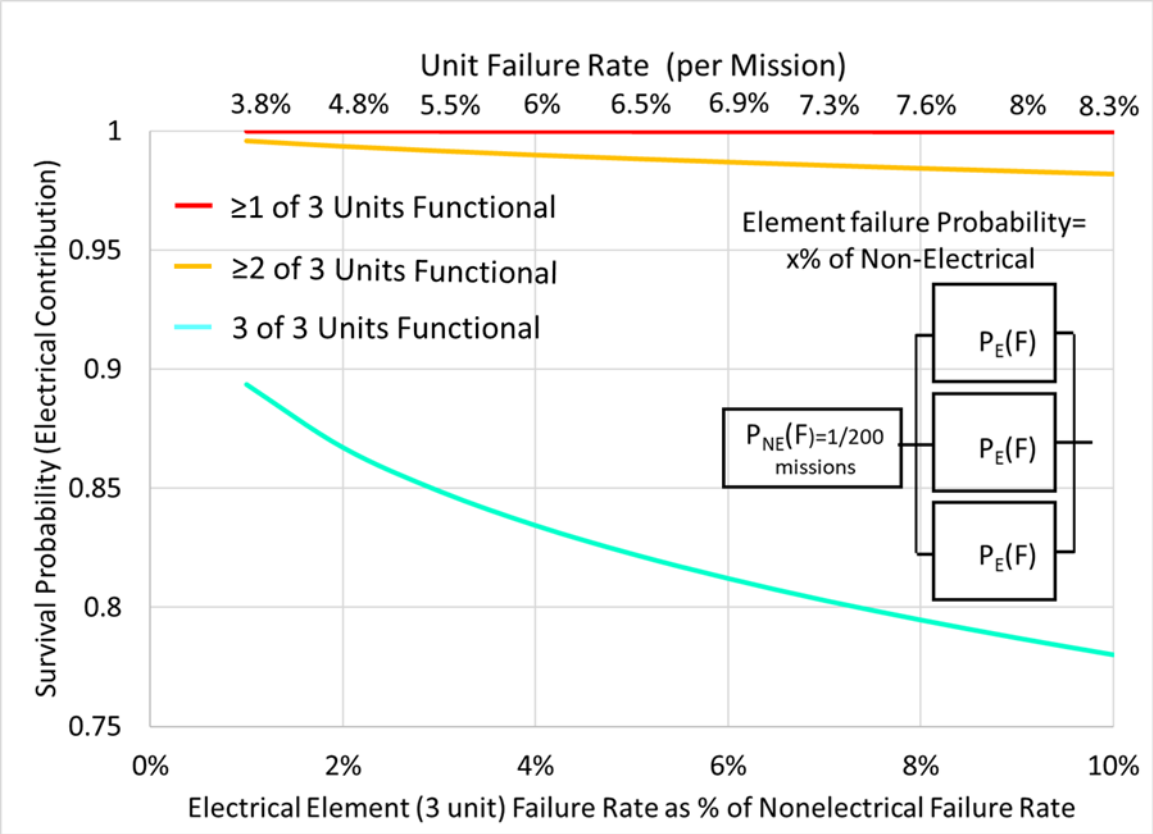


Figure 4. Probabilities of Retaining Voting, Comparison, and Service Availability (Note: All failure rates are per mission)

The unit failure rate on the upper x-axis corresponds to the electrical element failure rate (as a percentage of the 1-in-200-mission non-electrical failure rate). The red curve corresponds to the probability that at least one unit remains functional throughout the mission. It is much less probable that 2 of 3 units remain functional (which would allow detection of random errors in the units by comparing unit outputs—yellow curve). Still less probable is the situation where all three units in the element remain functional (turquoise curve), which allows errors to be detected and corrected by voting the unit outputs.

The purpose of adding redundant elements to a system is to ensure system-level success even as individual units fail. However, these failures affect system resilience, capabilities, and reliability. Loss of a single unit in a 3:1 system degrades system resilience with respect to survivability and availability while that unit is recovering. However, if the three strings are being used to vote out errors in individual elements, then a single-element failure results in loss of capability to isolate and correct errors. Therefore, a SEE can result in the system becoming zero-fault tolerant.

The impact of such degradation is application-specific. However, if the application is sufficiently important to merit redundancy to improve performance, then assessing the degradation of these system capabilities is warranted.

Moreover, if recovering (i.e., full operations) for the affected unit requires the system to be reset or resynchronized, each unit/box level error results in a temporary system-level outage. Using system-level redundancy to mitigate unit/box level SEE failures will degrade system-level strategies for performance and redundancy.

5.3 Redundancy Implementation to Mitigate SEE

Use of system-level redundancy to mitigate the effects of radiation, for transient errors and permanent failures, is a relatively new trend. Over the past seven decades, the susceptibility of electrical components to radiation has usually been addressed at the component level, independent from system-level redundancy implementation.

The components selected for the specific space environment were designed and tested to withstand the radiation level without experiencing transient effects or permanent damage. Unfortunately, the performance of such space-qualified parts significantly lags the most advanced commercial parts. As commercial electronics became more complex, their use in space environments resulted in a higher frequency of SEEs and new DSEE and NDSEE modes. Some commercial parts withstood radiation threats adequately while enabling essential performance advantages in their application. However, since the commercial parts were usually designed without consideration of radiation performance, it was impossible to determine which components would perform acceptably without radiation qualification efforts.

As demand for these higher performance components increased to enable the required functional performance, additional techniques were used to evaluate SEE. In simple cases of the various implementation of read-only memory (ROM) and random-access memory (RAM), these techniques would detect and correct single and double flipped bits on memory addresses. Some of these techniques (e.g., error detection and correction (EDAC)) could be checksums of large memory functions, or dedicated additional bits, to correct bit flips in memory. As each memory word was accessed, these additional bits would be used to detect, validate, and correct bit flips caused by a SEE in near real-time.

As circuits became more complex, with SEE affecting logic and decision gates within processors, application-specific integrated circuits, and field-programmable gate arrays (FPGAs), EDAC routines were not sufficient to detect all errors. In these cases, manufacturers of space-rated parts began implementing internal, component-level redundancy to address SEE-related errors. FPGAs employed internal triple-modular redundancy (TMR), where the function performed by the FPGA was replicated within the device and then voted by a radiation-hardened circuit to ensure the output would be correct in the presence of single errors.

Certain digital processing implementations employed SCPs, where computations were performed by two identical circuits and executed simultaneously to produce identical results. If the two outputs did not match identically, then an error would be detected and the process would be re-executed on a redundant pair of processors.

A critical point to all of these component-internal SEE mitigation strategies is that the radiation-induced error was handled at the component level. Specifically, any additional circuitry for this mitigation (e.g., EDAC bits, TMR gates, or dual SCP processors) were considered in the component's failure rates. This additional circuitry, employed to mitigate SEE, incurred a reliability penalty for those components. This internal SEE mitigation was automatically incorporated into the system-level reliability and availability model since it was included in the component-level failure rate.

When a subsystem box employs internal SEE mitigation strategies to address SEE-induced outages (e.g., error-correcting codes, internal voting), there is no need to use mission-level redundancy to back up critical functions. However, when a subsystem cannot repair SEE

internally, (e.g., processor exceptions and software crashes) some architectures employ mission-level redundancy to maintain critical functions. Repairing or restoring the subsystem sometimes necessitates resynchronizing redundant elements, resulting in temporary unavailability of all redundancies.

Mitigating SEE with system-level redundancy poses specific challenges, including:

1) SEE behavior in certain components involves multiple SEE modes with different consequences that may require multiple and diverse redundancy schemes.
2) Redundancy-based mitigation strategies are costly in terms of their effects on the system's SWAP.
3) Restoring full functionality after an SEE often requires taking the entire redundant system offline to re-set and resynchronize its constituent units.

Today's challenge is that when radiation mitigation has been elevated to the system level, the reliability impact of the SEE on system performance must be appropriately addressed in the system model, probabilistic risk assessment (PRA), and reliability model (e.g., Reliability Block Diagram, or RBD).

6.0 System Modeling

The NESC team started with a typical triple-redundant cross-strapped system architecture used in mission-critical applications. A standard RBD model was developed to characterize this architecture with representative failure rates for the electrical units. The error rates due to DSEE and NDSEE events were included for a subset of those elements. Representative repair times were added for SEE recovery of transient effects. The mission duration, functional criticality, and various operational constraints (i.e., 2 of 3 and 1 of 3 required) were considered in the analyses in Section 7.

6.1 Modeling Methodology

The NESC team chose a modeling approach to evaluate various SEEs on systems based on the comparative approach used in an earlier NESC assessment.[7] This assessment recognized that there is neither a "generic architecture" nor a "typical division" of failure rates between electrical and non-electrical system elements. No all-encompassing generic mission profile bounds mission-critical activities with natural and induced environments. However, to perform a quantitative analysis for this study, the NESC team defined an architecture and failure rate apportionment.

6.1.1 Redundant Architecture Description

Figure 5 shows the notional electronics architecture used for the relative comparisons as a simplified RBD[8] form for a system of three redundant subsystems. As in the referenced work, the notional architecture consists of 24 cross-strapped system elements (e.g., avionics boxes) in series, each with a baseline mean time between failure (MTBF) of 500,000 (500K) hours

[7] TI-12-00762, Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program (CCP), March 2012

[8] Reliability Block Diagram Modeling- Comparisons of Three Software Packages, Brall, A.; Hagen, W.; Tran H. 2007 Annual Reliability and Maintainability Symposium

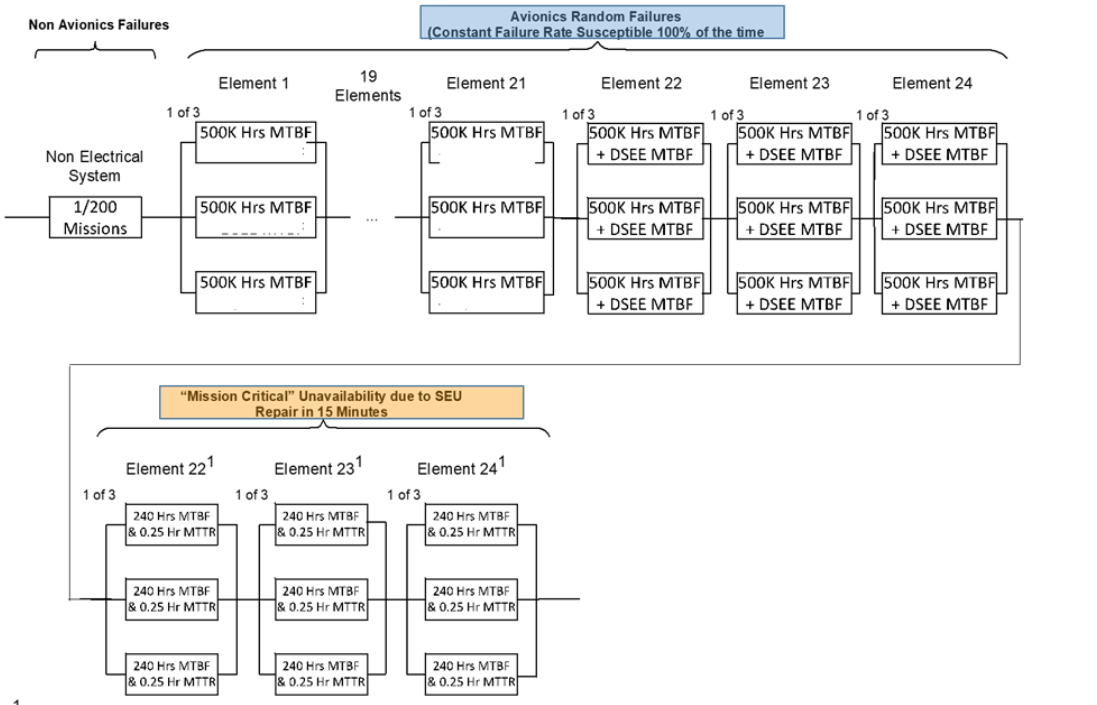
corresponding to a failure rate of $2x10^{-6}$ per hour. The origination of the 24-box architecture and the selection of a typical average failure rate is detailed in the footnote 8 reference.

The contribution of the non-electrical failures is depicted on the left of the RBD as a constant LOM rate of 1 of 200 missions. DSEEs are treated as a constant failure rate process, adding this rate to the 1 in 500K hours constant electrical failure rate for susceptible units. NDSEEs were treated separately and modeled as an availability prediction since they are reparable.

Figure 5 also shows the constant electrical failure rate (i.e., MTBF) of 1 failure per 500K hours plus the DSEEs, for susceptible units, in the blue section of the RBD. These constant failure rates apply for the duration of the mission. The standard reliabilty equation based on a constant failure rate over time $e^{-\lambda t}$ calculates the success probability. The figure shows NDSEEs as the orange section, with the last three system elements #22, #23, and #24 with NDSEEs.

The modeling approach to calculate the effects of NDSEE used the standard availability equation

$$A_I = \frac{MTBF}{MTBF + MTTR}$$



[1] Note boxes with identical unit numbers (22, 23, 24) represent separate and different failure rates and unavailability for each of the indicated units

Figure 5. Simplified Example Three-String Redundant Architecture

The modeling example used in this study divides SEE into two categories (reparable and irreparable). DSEE modes are non-reparable. NDSEE modes are reparable, provided the system has the resources and opportunity to repair them. The exception is for short missions or mission phases (i.e., <1 hour) where the mission/phase is too critical or too short to tolerate any system down time.

For missions longer than ~1 hour, NDSEEs are reparable, allowing the affected unit to resume operations after a finite repair time (T_R). The model varies the rate for reparable and non-reparable SEE (R_R and R_I) and the reparable time (T_R) to vary, while electrical unit failure rate (R_E) remains constant.

All 24 elements have a destructive constant electrical unit failure susceptibility with rate R_E. Units 22 through 24 have a constant DSEE rate and a nondestructive failure rate and repair time (i.e., the reciprocal of the MTBF and a mean time to repair (MTTR)) modeled as availability.

System-level non-voting architectures (e.g., 3:1 configuration) correct errors by "failing silent," allowing use of the outputs of the remaining two strings by the succeeding subsystem. If a second unit of the same element is lost, errors in the remaining element can propagate to the next system element.

System-level voting architectures (e.g., 2-out-of-3 configuration) correct errors by voting the outputs of the three strings after each element, providing results to the succeeding subsystem. If a unit of an element is lost to a SEE, then errors in one of the two remaining corresponding units results in total system loss due to inconsistent results between the remaining units.

The system-level model depicted in Figure 5 allows repair of nondestructive faults, allowing them to be treated as an "availability" term, shown in orange, in series with the destructive and other constant failure sources, shown in blue. This limits the impact of a nondestructive event to a single repair time. The model simulates the number of failures (i.e., three strings failed due to DSEE or accumulation of NDSEE) and the number of times failures and outages occur, and the average time spent with one or two strings failed as a function of DSEE and NDSEE rates, mission duration, and repair time.

6.1.2 Mission Phases

Figure 6 shows a simulated 30-day mission divided into several phases. The two red phases indicate 15-minute mission-critical periods where repair is not possible due to ascent and entry, descent, and landing (EDL) flight phases. During these mission-critical phases, repairing via "resynchronizing" or "rebooting" the system architecture is not possible, since repair strategies involve removing all redundant elements from the system.

The orange zone in Figure 6, starting at day 10 for 6 hours, indicates a mission-critical time period where a 15-minute repair period is possible, unlike the red zone. In this case, resynchronizing or rebooting the system architecture is possible, since removing all redundant elements from the system pauses the mission temporarily without LOM as long as the repair restores the impacted element within 15 minutes.

Figure 6's green zone indicates non-mission-critical periods where resynchronizing or rebooting the system architecture is possible because removing all redundant elements from the system has a temporary effect from the repair strategy. Even if all three strings are removed, the mission is not affected, since the system can be brought back after the 15-minute repair time.

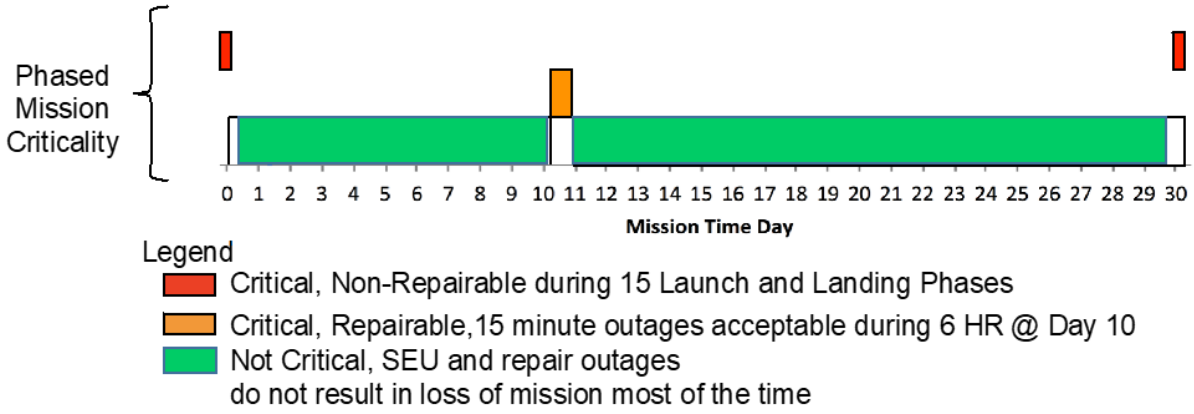
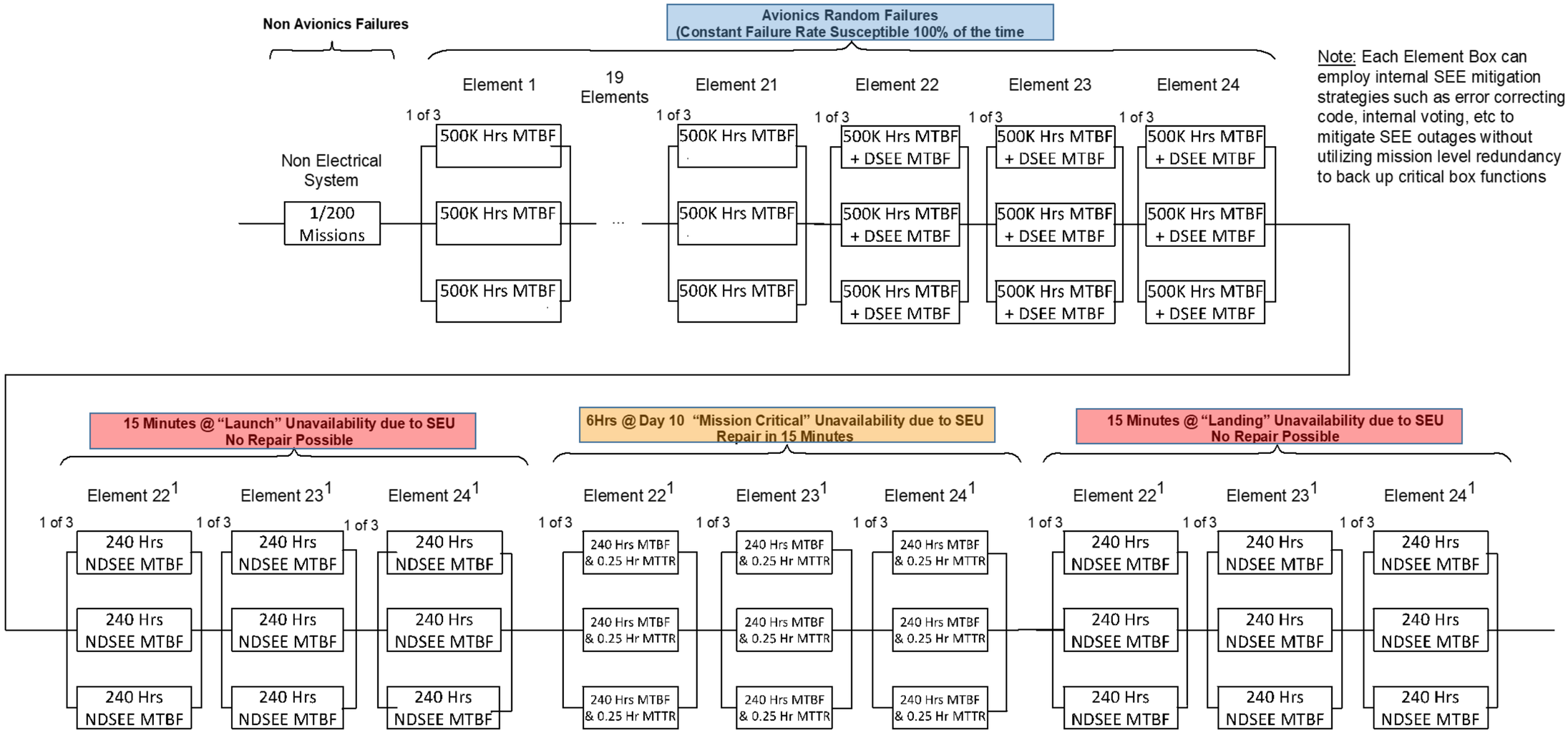


Figure 6. Assigning Avionics Criticality by Mission Phase

6.1.3 Integrating Mission Phases into the Model

This section applies the red mission-critical, orange mission-critical with repair, and green noncritical mission phases to various mission scenarios.

Figure 7 shows the fully integrated RBD model, with time-phased mission implementation. The non-electrical contribution of 1 of 200 missions is unchanged. The system is susceptible to random component failure and destructive events caused by radiation during the entire mission, as depicted in the blue segment. The two short non-reparable mission phases can be modeled as separate RBD blocks with limited time exposure, as depicted in the red phases. The mission-critical mid-time phase portion of the model can be implemented as a different RBD block, with repairs possible as an availability, as depicted in the orange section of Figure 8.



[1] Note boxes with identical unit numbers (22, 23, 24) represent separate and different failure rates and unavailability for each of the indicated units

Figure 7. Model of Constant "Destructive" Failure Rates plus the Three Periods of NDSEE (11x17 paper size)

System modeling efforts early in the design can use existing or historical SEE rates for parts in the system. For new systems with unknown SEE rates, system modeling can determine upper limits for SEE rates that would allow the system to operate successfully. These limits are useful during design and qualification processes.

The modeling approach described in this study investigates a range of DSEE and NDSEE rates, starting at low values and raising them until the system failure rate climbs into the unacceptable range. In parallel with varying the rates, the model can vary other parameters (e.g., mission duration, repair time). This allows determination of the SEE rate upper bounds as a function of model parameters, ensuring SEE occurring with other random errors will not overwhelm intended system redundancy strategies.

Based on a comparison of these upper bounds to what is known about the system and the SEE behavior of parts proposed for the system, modeling results provides guidance for prioritizing part level testing and analysis to reduce system risk most efficiently.

6.2 Mission Profiles

The system's operational use and the mission duration are as important as the system architecture during modeling of system-level consequences of SEEs. Section 6.1 describes three critical mission phases, each with specific usage strategies affecting system performance with respect to faults and SEE recovery. To consider these operational use cases and mission duration, the following sections describe examples of three distinct mission types.

6.2.1 Short Critical Mission Type or Phase (Red)

Figure 8 depicts a 30-minute mission duration with the first 15 mission-critical minutes (red zone) followed by a noncritical (green) phase. Mission-critical 15-minute phases are characteristic of a launch vehicle or a spacecraft performing a critical phase during an extended mission (e.g., on-orbit rendezvous with another spacecraft or EDL to an asteroid or planetary surface). During these short missions, the system requires active continuous system control. There is no opportunity to pause the mission, place the spacecraft in a safe mode, and reset (i.e., repair by resynchronizing) electronics that suffered a NDSEE. Therefore, all SEEs are non-reparable during the 15-minute red zone. During a mission-critical period, modeling the NDSEE failure rate involves applying the SEE MTBF as a constant failure rate for those 15 minutes.

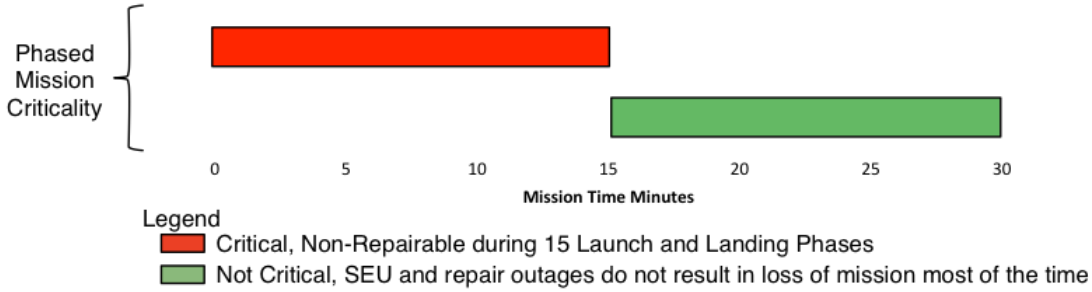


Figure 8. Short 30-minute Mission with First 15 Minutes Mission-Critical

6.2.2 Long Duration Critical Mission Type or Phase (Orange)

The next mission type represents a 1-year duration, as shown in Figure 9. During such a critical mission, shown in orange, mission success requires continuous system performance or a type of

satellite. This mission phase could pertain to a communication satellite, where the instrument must continually monitor and transmit its signal, or to an Earth-observing or weather satellite that must continually monitor the Earth's atmosphere.

These missions require the system to operate continuously, regardless of the rate and consequences of SEE. During this mission-critical phase, redundant elements must remain operational even when SEE occurs. As long as at least one of the three redundant units within each element remains operational, the mission continues to operate successfully.

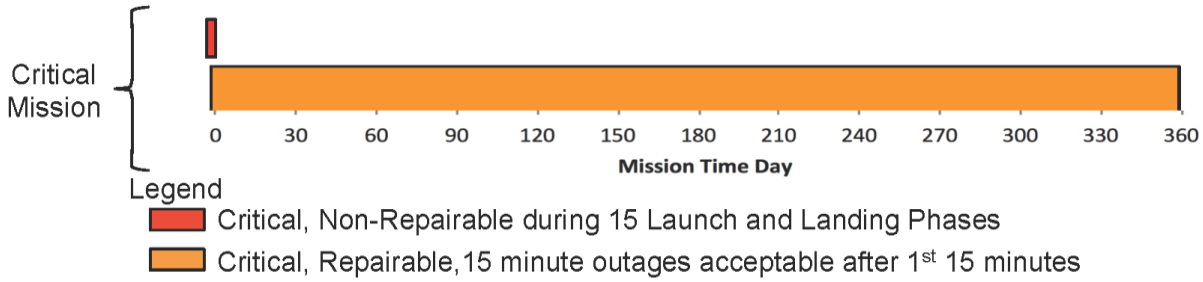


Figure 9. Long Duration Critical Mission

6.2.3 Long Duration Noncritical Mission Type of Phase (Green)

The last mission phase, or type shown as green in Figure 10, represents a noncritical phase where repair can involve a resynchronization or rebooting of SEE susceptible elements. This is an application requiring the system to operate at certain times of the mission, but having long phases of transit or mission operations that do not require active control or monitoring.

Examples include a mission where the loss of a complete subsystem due to a combination of reparable SEE and failure (for any reason) would not result in the system loss. This could be a failure of the navigation or control system during quiescent flight, where no active control is essential. It could mean the temporary loss of the environmental control and life support system where the existing reserves on the spacecraft are sufficient to sustain the system during the temporary outage.

Such events could result in LOM performance for a time period, but would not cause a complete system loss. Although the subsystem is disrupted by a SEE, in these cases the system returns back online with a function recovery and reset. Moreover, if multiple SEEs cause the system to fail, it will recover after a system reset and continue its mission. This same type of mission phase applies for a critical mission (i.e., a science mission) requiring continuous service. In this case, although the service is disrupted and observation time is lost, the entire system is not lost and functionality, along with the lost opportunity, is recovered after a system reset.

The distinguishing characteristic of this mission phase is its reduced susceptibility to reparable SEEs. Such events result only in those temporary anomalies resulting in a system outage followed by restoration of on-orbit service continuing the mission.

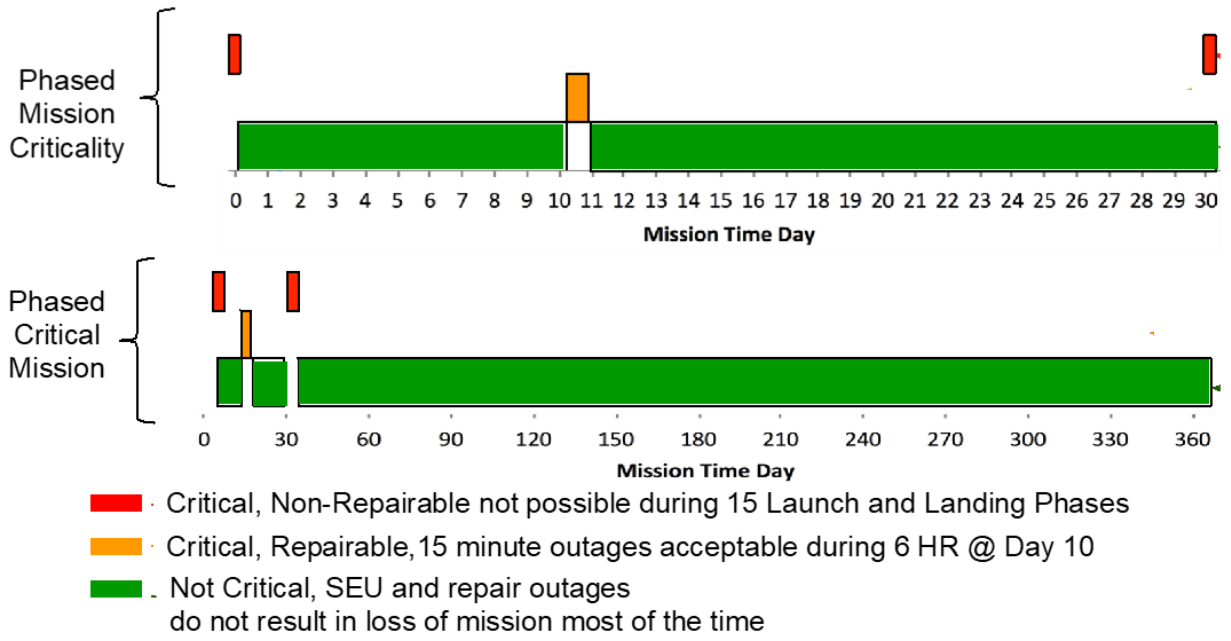


Figure 10. Long Duration Not-Critical Mission with Mission-Critical Periods

6.2.4 Time-Phased Missions (Red, Orange, and Green)

The modeling done for this study investigated the effects of SEE on a time-phased mission. Figure 10 shows a sequence where system criticality changes during the mission. Consider an ISS visiting vehicle, required to rendezvous with a human-inhabited outpost to replenish supplies and return the crew to Earth. This is a 30-day mission with multiple phases.

The first phase includes a mission-critical (red) liftoff and ascent phase to low Earth orbit. This red phase is representative of a short mission duration where no repair is possible. The requirements and performance of this phase are commensurate with the implementation described in Section 6.2.1. The system must continually operate with no disruption of service and without component recovery.

The second phase of the mission includes a multi-day transit to the ISS or other outpost, shown in green. During this time, the spacecraft is mostly on a minimally controlled trajectory path to the rendezvous location with no continuous active control required for safety-critical functions. If a SEE caused a temporary upset in a function (i.e., the attitude control subsystem), then a reset and resynchronization of the subsystem would fully restore its functionality. This phase of the mission is representative of a long duration, noncritical part of the mission, and the success expectation is modeled as described in Section 6.2.2. The complete system outage is allowed as long as recovery of the lost function is possible.

The third phase of the mission represents a highly active mission requiring continuous system operation, shown in orange. This phase includes proximity operations and rendezvous phase of the spacecraft to the ISS or a similar outpost. During this phase, the system must remain operational with no disruption in service. The attitude control system cannot experience a temporary outage of service, since an uncontrolled spacecraft in this vicinity could result in a collision. However, SEE repairs and recovery are possible during this phase since there are typically hold and safe states during the phase that allow for subsystem reset and recovery.

Although these systems require a level of redundancy for fault tolerance and safety considerations, as long as a single string of the system remains operational during this time period, the system remains functional. When all three strings of the subsystems are lost, due to failure or consecutive SEE upsets, the subsystem outage results in system loss. This phase of the mission is considered a critical mission phase, and the performance expectation is described in Section 6.2.3. One operational string is necessary at all times, with failed elements returned on line within the specified repair time.

The next phase of the mission represents a docked condition where the vehicle is physically attached to the remote output and not required to support continuous noncritical green operation actively. Alternatively, it could be a second transit phase of the mission, where the vehicle is no longer in proximity to the outpost and transitioning to a new location. In these applications, a temporary outage of any function would not result in a LOM. This would be identical to the system performance described in Section 6.2.2.

The final phase of the mission includes EDL as the spacecraft returns to the Earth or descends to another planetary body. This is similar to the short mission phase described in Section 6.2.1, where the system functions are critical and need to be continuously operational. This operational restriction precludes the ability to repair or recover lost assets due to a temporary error. Any loss of the required function, even temporarily would result in a system loss.

The effects of combining these distinct mission phases into a comprehensive mission profile and the resulting mission performance expectation is illustrated and discussed in Section 7.

7.0 Results and Discussion

The results presented are based on the models discussed in Section 6, where the non-electrical and non-SEE upset rates were held constant. The NESC team analyzed the sensitivity of these simplified models to various parameters, including rates for reparable and non-reparable SEE modes, repair time for reparable modes, and mission duration. The team examined the probability of system failure as a function of the distribution of reparable and non-reparable rates across the sensitive avionics units (i.e., 22 through 24 in the three redundant strings), as shown in Figure 7.

7.1 System Modeling Results

First, the NESC team evaluated the importance of mission lifetime, beginning with very short missions or mission phases where repair of NDSEE modes is not possible. Then the team examined how the probability of suffering system outage increases as a function of the mission lifetime and operational requirements.

7.1.1 Very Short Mission Durations

During very short missions or mission phases (e.g., 15 minutes), operations may be too critical, and the mission duration too short, to allow for repair of NDSEE and other potentially reparable faults. Missions of this type include launch, EDL to Earth, and in some cases, operations in proximity to another space vehicle or astronomical body. For such missions, any error or failure mode is effectively irreparable. Because NDSEE modes typically occur at rates orders of magnitude higher than DSEE, these NDSEE modes will dominate the unit and system failure rates.

For such short missions, non-electrical failures dominated the system failure probability and were constant at 1 in 200 missions. Electrical failure rates were constant at 500K hours MTBF in units 1 through 24. The SEE failure rate was varied to investigate the impact of these rates on the system failure probability. Figure 11 illustrates that SEE would have to occur at a rate of about 2 to 2.5 per day per unit to reduce mission success probability by 1% below that due to non-SEE causes.

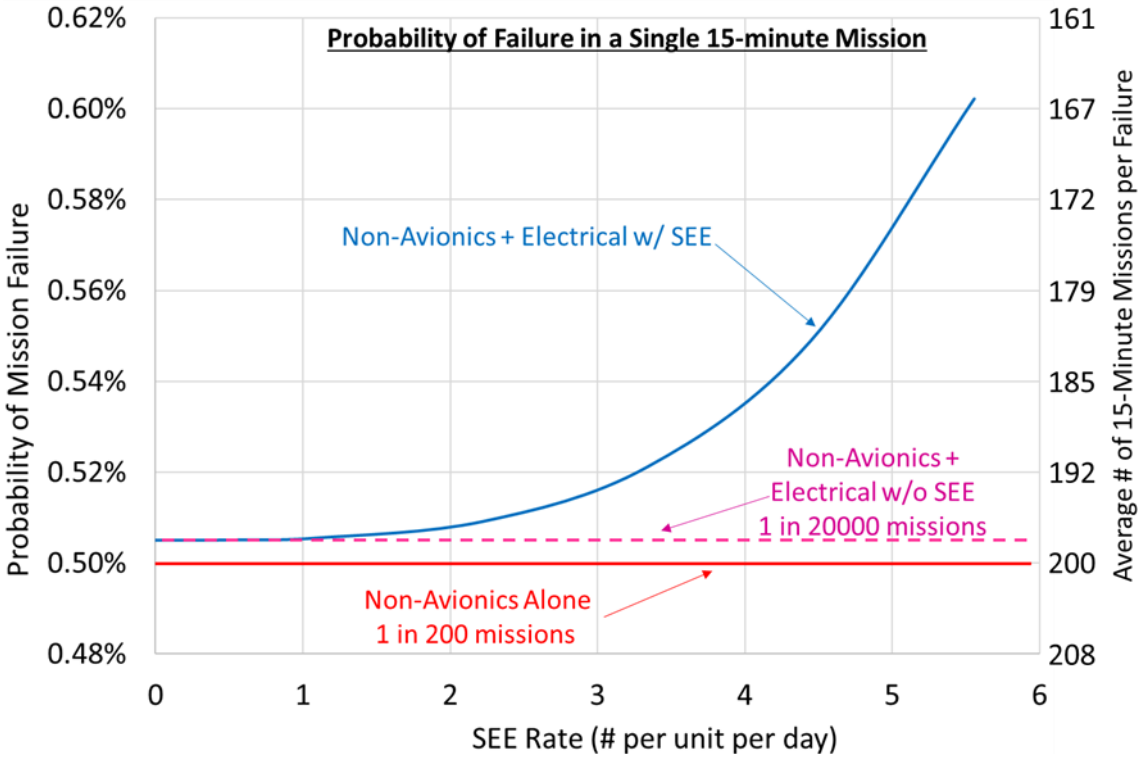


Figure 11. SEE Rates Would Need to be High (>1 per day) to Significantly Impact Failures for Short Missions

7.1.2 Longer Missions

The probability that at least one SEE occurs increases with mission duration. This means SEE-induced failure probabilities are more likely to be commensurate with or even exceed non-avionics failure probabilities for longer missions.

Moreover, because of uncertainties on SEE rates due to incomplete SEE characterization testing, the system SEE failure rate may not be known with precision. For this reason, the NESC team examined how system outage rates respond to variation of key model parameters.

The NESC team began by looking only at reparable SEE modes. The team assumed when a SEE takes a unit offline (e.g., one unit of element 22), the system continues to operate, with the remaining instantiations of that element's unit filling in for the affected string. After a nominal repair time, the affected unit is returned to service and the system functions nominally. Only if all three units in any single element (e.g., element 22) are affected by SEE during a single repair time does the system experience a service outage. The consequences of the outage depend on the application. The outage may recover automatically; it may recover after intervention by ground

systems after a nominal outage time; or the outage may be irrecoverable. For this study, automatic recovery was assumed.

As long as the repair time is sufficiently short and the reparable rate is sufficiently low, the probability of accumulating three SEEs in a single repair interval is negligible compared to the 1-in-200-mission non-electrical failure rate. However, as mission lifetime increases, there are more chances for such an event to occur, much as the chance of rolling snake eyes with a pair of dice increases with the number of rolls. Figure 12 illustrates how the probability of a system outage increases as the mission duration lengthens over a range of SEE rates and repair times, with a constant electrical failure rate. Because recovery is assumed, Figure 12 illustrates the outage probability differences due to reparable SEE.

The reparable SEE rate (R_R) for each unit varies from 0.055 to 0.22 per day. Three repair times (T_R) (e.g., 6, 18, and 60 minutes) were reviewed.

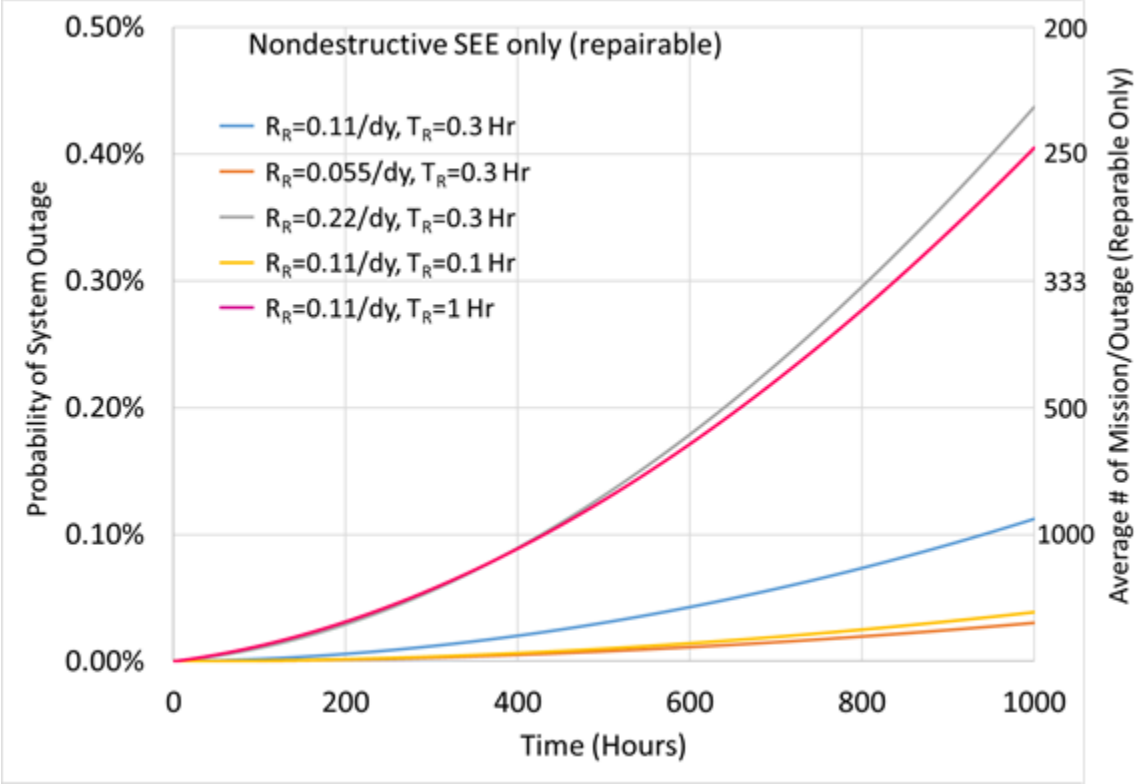


Figure 12. Outage Probability as a Function of Reparable SEE Rate and Repair Time

As mission duration increases, SEE can become a significant driver of system outages even when they are reparable. Figure 13 shows the trend extended to mission durations of 10K hours. Note that the nonlinear increase in outage rate with mission duration arises because the system is still susceptible to electrical failures at a rate of 1 in 500K hours per unit.

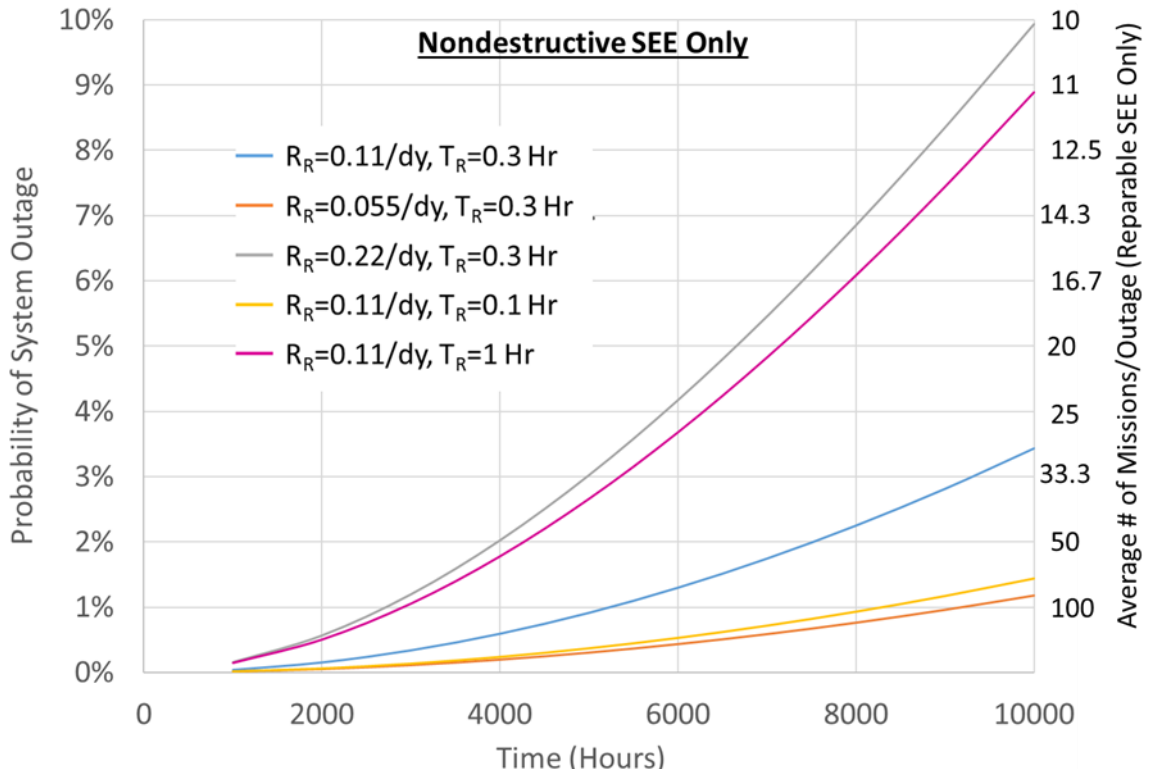


Figure 13. System Outage Rate vs Reparable SEE Rate and Repair Time for Longer Missions

From Figures 12 and 13, the SEE rate and repair time are important in ensuring reparable SEEs do not compromise mission success, especially as mission lifetime increases.

The influence of irreparable SEE was discussed for very short missions. As mission lifetime increases, the increasing probability of such events can affect mission success and resilience if they occur at a sufficiently high rate (see Figure 14).

Figure 14 shows system failure probability as the rate of irreparable SEE increases from 0.0011 to 0.0055 per unit per day. System outage rates rise nonlinearly with unit DSEE rates.

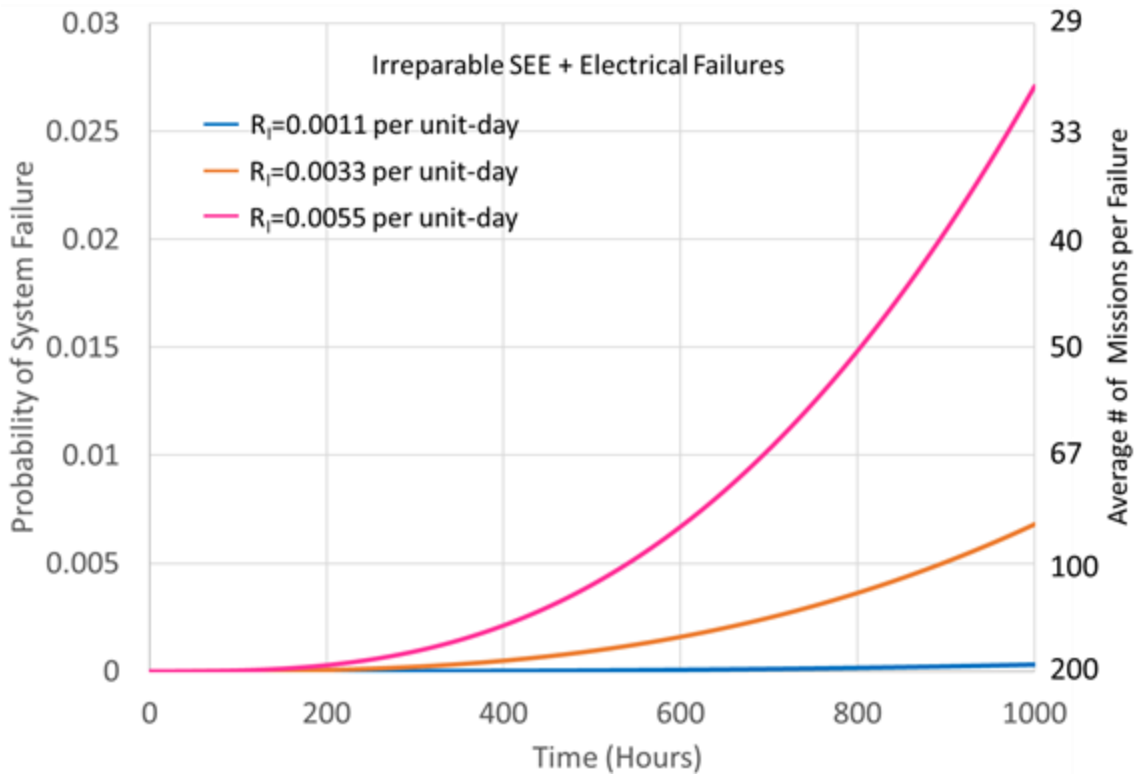


Figure 14. System Failure Probability as Rate of Non-reparable Rates Increases

When reparable and irreparable modes occur, the mission length becomes more important. This is because the probability of an irreparable SEE mode accumulates over time, increasing the likelihood that the system is less resilient to NDSEE near the end of life. (See Figure 5).

Because outages in a redundant system require multiple failures, the probability of such outages increases nonlinearly with mission lifetime and reparable and irreparable SEE rates. The probability of outage is approximately linear with repair time.

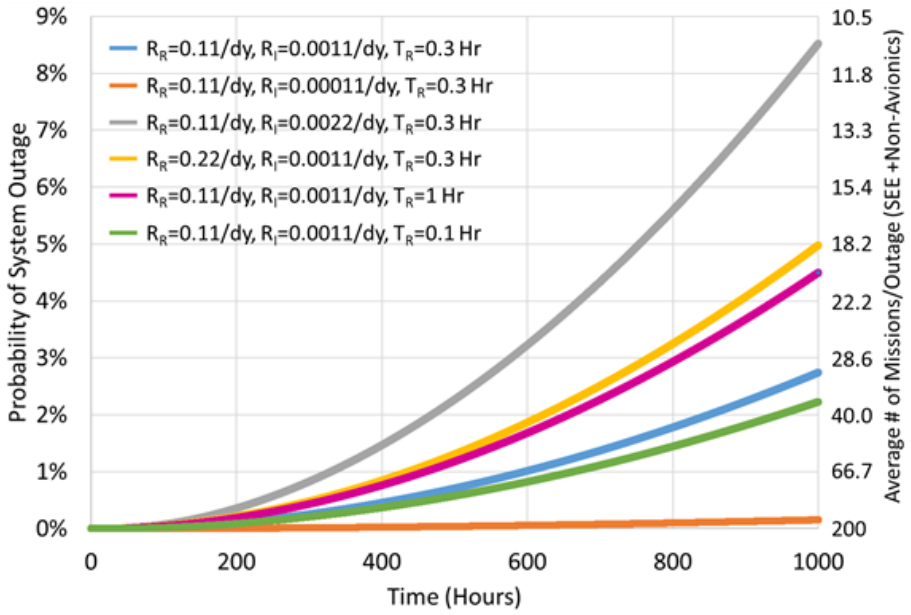


Figure 15. Probability of System Outage Occurring During 1000-hour Mission Due to Reparable and Irreparable SEE

As noted, the cross-strapping of SEE-susceptible avionics units means outage probability is driven by the most sensitive unit rather than by average sensitivity. Figure 16 explores how the distribution of reparable and irreparable errors among units 22 through 24 affects outage probability. The irreparable SEE rate plays a significant role in driving system outage probability.

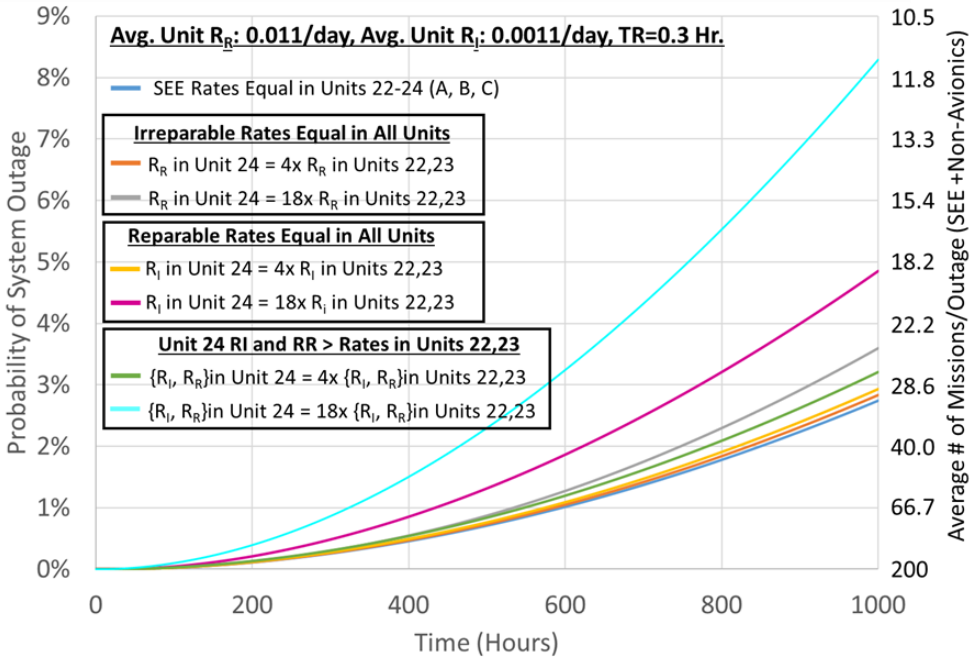


Figure 16. Dependence of System Outage Rate on Distribution of SEE Rate Throughout Susceptible Units

The weakest unit in a cross-strapped architecture drives the system failure rate, especially if redundant units are identical.

7.1.2.1 System Degradation due to SEE

Although these analyses have been concerned with system outages, the loss of one or more units within an element can have important consequences for the mission. Exactly what these consequences are depends on the system application and the tasks being performed by the redundant units. At the very least, temporary or permanent loss of a unit reduces the resilience of that system to errors and failures.

If, in addition to ensuring system availability, the redundancy is being used to correct errors that occur in the units that make up each string, then system performance can be compromised. For example, Element 22 has three units (i.e., 22A, 22B, and 22C). The cross-strapping in the system allows unit 22B or 22C to fill in while unit 22A is offline. However, if an error causes a disparity in output between 22B and 22C, it would be unclear which unit was correct. Even if these units had the ability to compare outputs, they would not be able to isolate and resolve the error.

Moreover, the recovery after an outage in a unit may require taking the system out of service for a nominal recovery time to resynchronize the redundant elements. Given these possible impacts, it is useful to consider the expected time that errors and failure modes may result in one or more electrical units experiencing an outage during a 1K-hour mission. Table 1 shows the expected totals for events and resulting periods of unit outages for the three contributors: non-radiation causes (i.e., 1 per 500K hours for each of the 72 units in the model), irreparable SEE (1 per 900 days per electrical unit), and reparable SEE (0.11 event per day per electrical unit, with an 18-minute repair time).

Table 1. Expected Unit Outages and Failures and Their Consequences for 1000-Hour Mission

	Non-Radiation 1/500K hours per unit	Irreparable SEE 1/900 days per electrical unit	Reparable SEE 0.11 event per day per electrical unit; 18 min. unavailability per event
Expected # per 1000 hours	0.134	0.34	41.67
Mean time in degraded Condition	68.7 hours	182 hours	12.5 hours

The most obvious aspect of the entries in Table 1 is that the amount of time the system is in a degraded state due to reparable SEE is significantly less than other causes. Although irreparable SEE and non-radiation errors occur much less frequently (i.e., less than one expected per mission) the system outage time is greater. This is because the outage duration for reparable SEE is limited to a single repair time, while outages for irreparable SEE and non-radiation failures last from when they occur until the end of the mission.

7.1.3 Phased Critical Mission

Next, consider the effects of SEE to the system success probability over the entire mission timeline, where the operational system requirements change over the mission duration. For this portion of the study, the NESC team assumed that the DSEE rate in all units is negligible compared to the electronics failure rate of 1 per 2 million hours. Figure 18 illustrates a 30-minute mission where the first half of the mission operation does not allow repair, and the second 15 minutes allows for SEE recovery. An example of such a mission would be a launch vehicle's upper stage, where the avionics must continuously control the vehicle during ascent and then, after achieving orbit, has a small quiescent time period to recover from anomalies before another orbital burn is required.

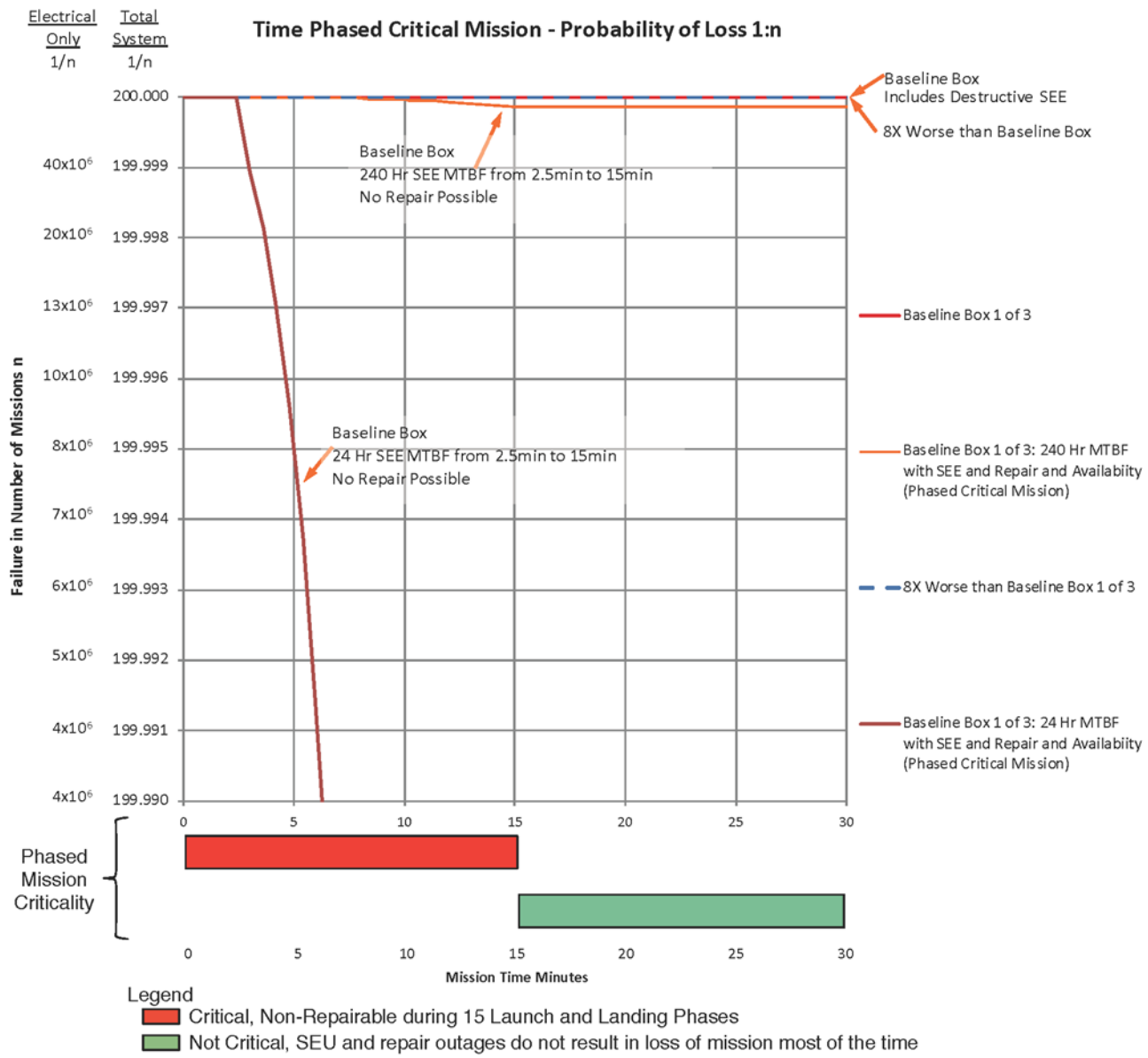


Figure 18. LOM and Electronics Failure Rate: First 30 Minutes

There are two scales for the y-axis; the leftmost scale depicts the probability of losing all three electrical strings during the mission time. This outer scale depicts one loss of electrical components given between 4,000,000 and 40,000,000 attempts. The inner scale depicts the LOM probability from 1 loss in 199.99 attempts to 1 loss in 200 attempts.

The plot illustrates the effects of three different failure and SEE rates for the same system architecture, as described in Section 6.

The red line at the top of the chart shows the results of a baseline system that does not experience SEE-induced transient upsets.

The blue line illustrates a similar system that implements lower grade parts (with failure rate 8 times higher) than the baseline system. This would be a system that does not employ space-

qualified parts, but uses military or industrial grade parts with a lower MTBF (but ignoring SEE susceptibility).

The orange line depicts the same architecture and operations, but uses the higher quality parts as in the baseline system and also considers the effect of transient upsets caused by radiation. The rate at which the upset occurs is assumed to be 1 upset per unit every 240 hours.

Three key items should be noted from Figure 18.

1) There is a relatively small effect to the component failure rate over such a short duration mission with this level of redundancy, when SEEs are not considered.
2) The SEE influence on system probability has a greater impact than the part quality.
3) The main contribution of SEE to the system failure rate occurs during the active mission phase (i.e., red), where recovery is not possible. Once the system enters the phase where recovery is allowed (i.e., orange), the rate of decreasing mission success is consistent with the rate of system success where SEEs are not considered.

The third point indicates that when SEE errors occur during a mission phase that makes their recovery impossible or difficult, SEE rate and time of exposure contribute significantly to mission failure probability.

Figure 19 plots a 30-day mission and illustrates the rapid increase in system failure probability due to effects of SEUs during time-critical ascent and entry mission phases.

The same redundant architecture is considered with different assumptions on the component failure rate and the SEE upset rate. The y-axis contains the same two scales depicting electrical failure contribution and total system failure. The x-axis has been extended to the 30-day timeline with critical non-reparable phase (depicted in red), noncritical reparable mission phases (depicted in green), and critical reparable phases (depicted in orange).

The red line at the top of the figure shows the baseline system neglecting SEEs. The second solid purple line illustrates the baseline system, where reparable SEEs are considered. SEEs were assumed to occur at 1 upset per 240 hours per unit, and the recovery of the upset component is completed within 15 minutes. SEEs have a minimal effect on the 1 of 3 system failure probability.

When the SEE rate increases to 1 upset every 24 hours there are three significant drops in the system reliability, as seen in the brownish third line, the upper line with steps. The first and last occurred during the 15-minute phase where SEE recovery was not possible. This would be expected since the high rate of SEE overwhelms the system redundancy. A notable result of this analysis is the significant increase in the system failure probability that occurs during the 6-hour critical mission phase where SEE recovery is possible. This is important to consider when using SEE susceptible parts that must continue to provide critical functions. Depending on the SEE upset and recovery rate, these contributions can have a severe detrimental effect to the system probability.

The fourth dashed blue line compares the effects of using significantly worse parts, neglecting SEE. This plot shows a purely continuous decreasing trend to the system probability that is driven by the constant failure rates of the units.

The fifth curve (i.e., orange) depicts the results when the SEE rate is doubled to 1 upset every 12 hours. The more dramatic SEE contribution to mission failure is illustrated in Figure 19 and indicates the importance of being able to bound the SEE rates. This plot illustrates where SEE susceptibility in high-quality parts will provide a higher risk than using lower grade parts (neglecting SEE susceptibility).

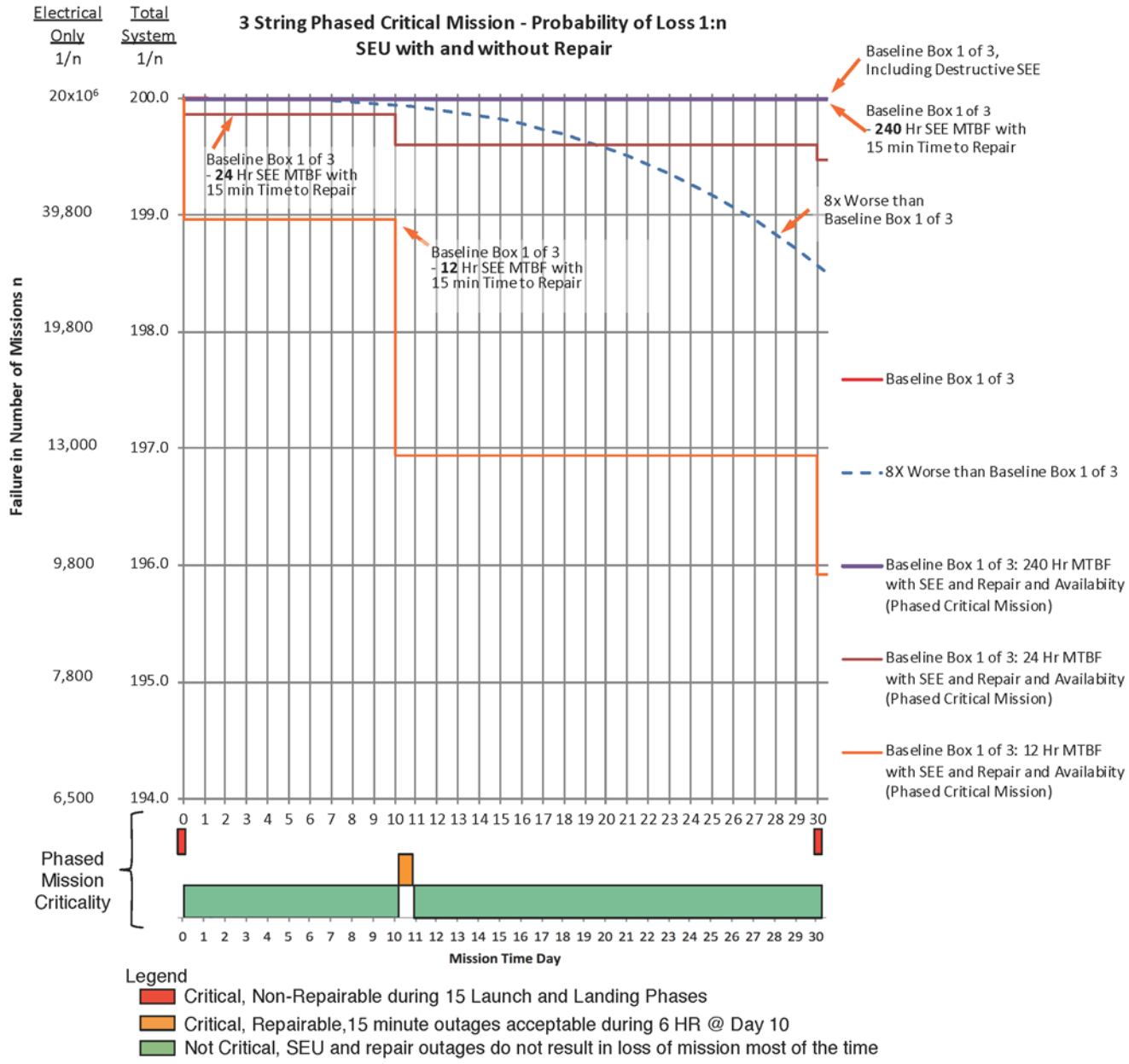


Figure 19. LOM and Electronics Failure Rate: First 30 Days

Figure 20 extends the 30-day mission to 365 days to illustrate the effects of the SEE over an extended exposure. The different upset and recovery rates remain the same; only the time line has changed. The identical step drops during SEE exposure are evident, and the exponential system decay probability subsequent to these SEE-induced operational constraints is illustrated.

This chart shows that after the SEE susceptible mission phases are complete, the system failure is driven entirely by the component failure rate and the part grade can have a significant influence over longer mission duration.

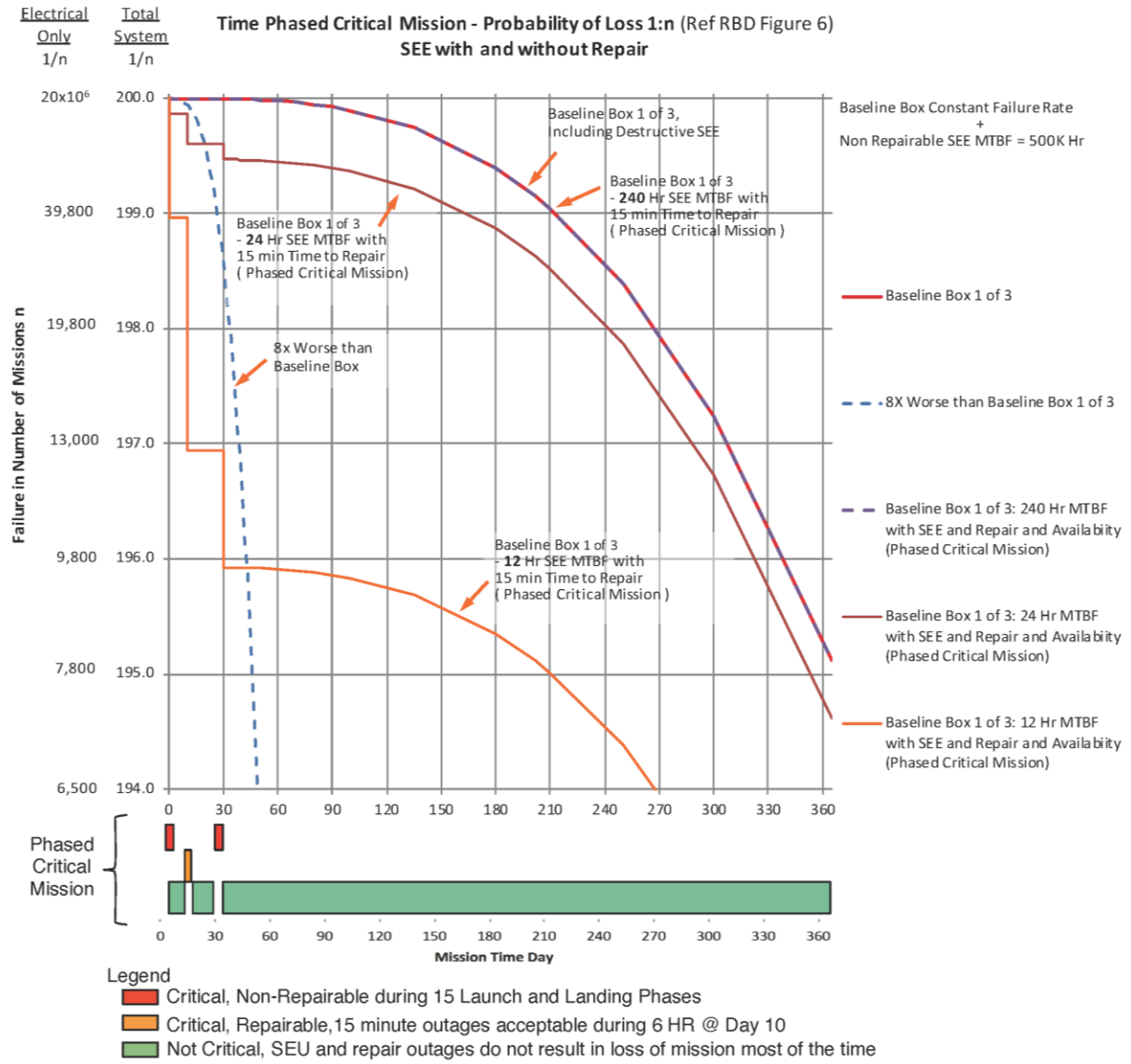


Figure 20. LOM and Electronics Failure Rate 365 Days with SEU Repair

Figure 21 shows the results of requiring at least one string to be operational at all times. There is no quiescent period where the system outage will not affect mission success. In this example, only the first 15-minute phase is considered non-reparable. After this initial phase, all transient SEEs are reparable with the 15-minute recovery time. As long as the recovery time is two orders of magnitude quicker than the expected upset rate, the effect on LOM is negligible. In this mission example, the effects of the SEE on the LOM are driven by the 15-minute non-reparable phase.

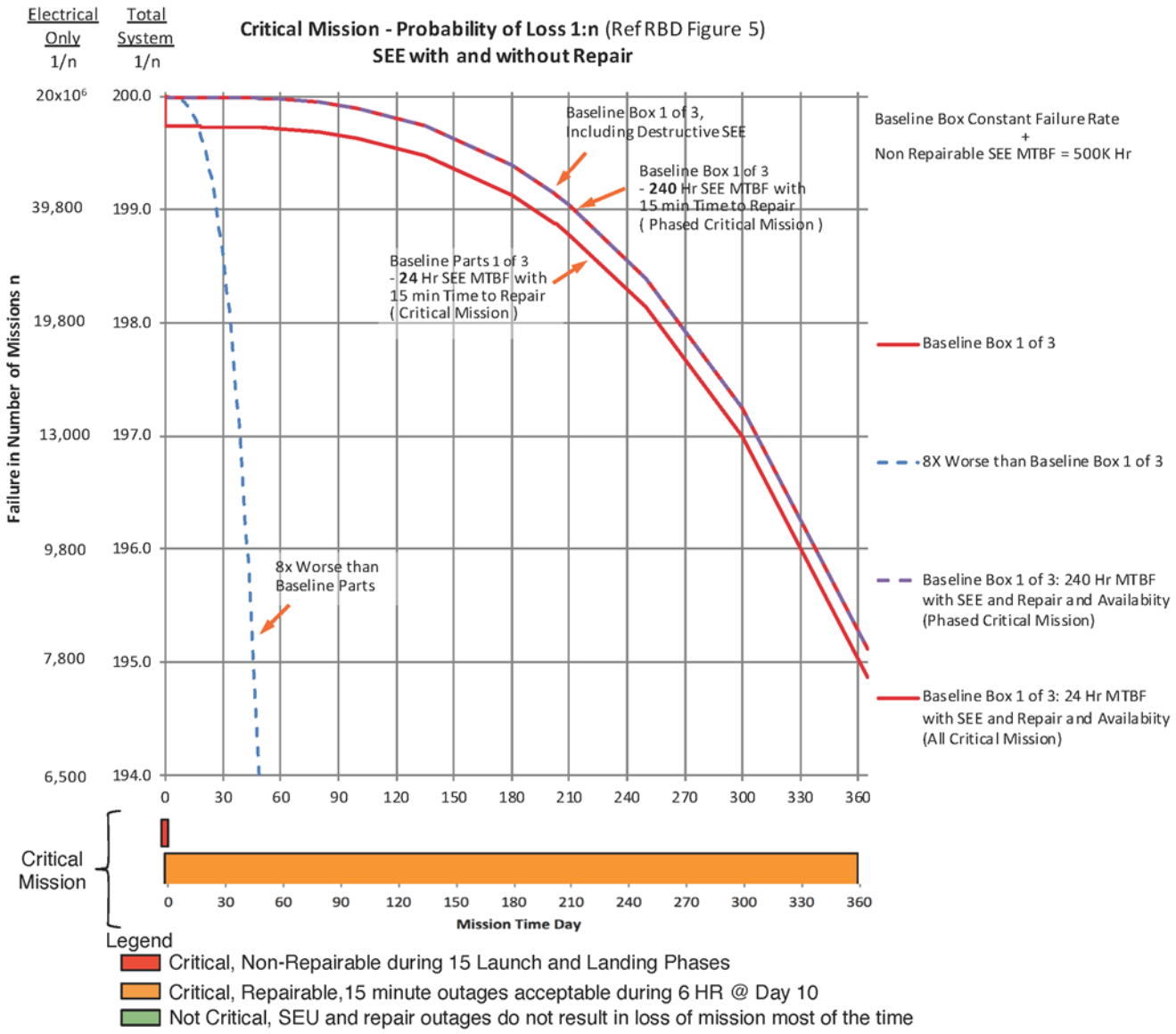


Figure 21. LOM and Electronics Failure Rate 365 Days with SEU Repair

7.1.4 Comparison of SEE on Different Architectures

Figure 22 compares the case of zero SEE rate to that where the SEE upset interval and subsequent15-minute repair create a 1% increase on LOM for various system-level architectures.

Figure 22 assumes a 100% mission-critical scenario and compares several architectures, includng: 1 of 3 cross-strap, 2 of 3 cross-strap, and 1 of 3 block redundant architectures over a 30-day and a 1-year time span. In addition, the effects of a nominal EEE destructive failure rate for all parts and a failure rate 8 times worse for all EEE parts in all units are considered.

Using the modeling techniques described in Section 6, relative comparisons show several interesting relative results illustrating the dramatic influence of system architectures on the interval between mission failures:

1) In a 1 of 3 cross-strapped architecture, parts with destructive failure rates 8 times worse than the baseline results in the same mission level degradation as having 1 of the 24 elements knocked offline for 15 minutes by an SEE every 8.3 hours, or 3 of 24 elements experiencing 15-minute outages for SEE every 12 hours.
2) For a 2 of 3 cross-strapped architecture, experiencing an upset every 102 hours decreases the interval between mission failures by 1%, while the 1 of 3 block redundant architecture requires an upset every 12 hours to reduce its mission-failure interval by the same 1%.
3) A 1 of 3 cross-strapped system has similar decrease in mission-level failure interval from 30 days to 1 year time span. A 2 of 3 cross-strap system and a 1 of 3 block redundant system have similar failure interval reduction as a 1 of 3 system for the shorter 30 day mission, but the latter has a much lower interval between failure for a 1 year mission (1 in 22 to 38).

Figure 22 shows how different architectures have dramatically different tolerance to reparable upset rates.

Comparison of 100% Critical Mission with 0 SEE Case to the SEE Interval Creating a 1% Increase in Loss of Mission

Units = 1/n Mission Loss @ Hrs SEE MTBF assuming 0.25 Hr MTTR

Number of Susceptible Elements out of 24:	30 Days			1 Year		
	0 SEE	1 Element	3 Elements	0 SEE	1 Element	3 Elements
1 of 3 Cross-strap System:	200	198@8.3Hrs	198@12Hrs	195	193@8.3Hrs	193@12Hrs
1 of 3 Cross-strap System 8X:	198			17		
2 of 3 Cross-strap System:	194	192@59Hrs	192@102Hrs	38	37.8@25Hrs	37.8@45Hrs
2 of 3 Cross-strap System 8X:	74			2		
1 of 3 Block Redundant:	198	196@8.3Hrs	196@12Hrs	22	21.8@3.8Hrs	21.8@5.6Hrs
1 of 3 Block Redn System 8X:	52			1.1		

Recoverable SEE in 1 or 3 redundant elements can degrade System Level Reliability as much as 8 x worse parts in all elements with no SEE

Architecture choices affect SEE rates resulting in significant (8x) reliability impacts

Figure 22. Comparison of SEE Rates and Architectures Resulting in 1% Reliability Degradation

7.2 Implications of Modeling Results

The preceding analyses have focused on:

1) Developing methodologies for including irreparable and reparable rates (with anticipated repair times) in system-level risk modeling to ensure the radiation effects in electronics are not a significant mission risk contributor.
2) Applying the results of parametric system-level risk modeling to guide the SEE component test and analyses efforts to ensure the limits used in the model are bounding.

In addition, several trends and conclusions emerge from the modeling results of Section 7.1.

1. The additive nature of failure rates in a series system means different causes impact system outage and failure probabilities in proportion to these rates.

a. Example: if a system has a non-electrical failure probability of 1 in 200 missions and SEEs cause 1 in 20,000 missions to fail (i.e., 1% of the non-avionics causes), the expected missions between failures reduces from 200 to 198 (a 1% change).

b. The additivity of SEE rates also means that in the absence of test data to the contrary, the unit rates for destructive and nondestructive SEE increase with the numbers of potentially susceptible parts used in the unit.

2. Because multiple component failures must occur to cause failure in a redundant system, system failure probability increases nonlinearly with the component failure rate. This has several implications for the triplicate system studied here:

    a. System failure probability increases quadratically with the unit failure rate, including the SEE contributions.

    b. Even when the probability of accumulating multiple SEEs in a single repair time is small, the probability of such accumulation is not negligible if the mission is long enough (i.e., contains enough repair times).

    c. The system outage rate due to reparable events decreases linearly as repair time decreases.

    d. Outage and failure probabilities increase quadratically with mission duration, due to accumulation of random failures due to DSEE and other causes.

3. For missions or mission phases where repair of NDSEE is not possible, all SEE modes cause a unit to go offline, and NDSEE dominate risk due to their typically higher rates.

    a. Short missions (e.g., launch vehicle) typically do not last long enough for SEE to accumulate and overcome redundancy. However, SEE can be the most significant cause of unit failures, degrading resiliency and/or capability and lowering mission success probabilities to unacceptably levels.

    b. For longer missions, a short mission phase where repair is not possible can significantly reduce the probability of mission success.

4. When cross-strapping is used to improve system reliability, it is important to bound the SEE rates for the redundant units to ensure that the SEE rates do not dominate the element failure probability.

5. If redundancy is used for different purposes, then the level of redundancy in the system may differ for those functions.

    a. Example: a 3-unit element can be used to ensure system availability and to correct SEE occurring in its units. The former has a 3:1 redundancy, while the latter function requires all three units to remain functional, so there is no fault tolerance for handling the SEE error correction.

    b. Example: Similarly, if the redundancy serves FDIR/voting purposes, then system availability will be reduced because SEE mitigation and FDIR often require the system to be removed from service for a repair time to resynchronize after a reparable error.

The above trends also suggest the following guidelines for system-level modeling and the use of modeling results to guide SEE test and analysis efforts.

7.2.1 System Design, Modeling, and Analysis

The following guidelines are suggested to maximize the value of system-level modeling for design and SEE testing and analysis efforts:

1) Irreparable and reparable SEE rates should be included in system models.
    a. If a quantitative reliability assessment is used (e.g., RBD or PRA), then the SEE rates should be combined to the component or unit failure rates.
    b. Reparable SEE can be assessed using availability modeling by including the SEE rate and system repair/recovery times.
2) Investigate the reliability and availability model sensitivities over a range of rates for reparable and irreparable events and recovery times to determine the level at which they significantly detract from mission success.
    a. In most systems, the non-electrical failure rate dominates and provides a natural scale for measuring the significance of failures arising due to DSEE, NDSEE, and other electrical causes. It is natural to define "significance" as a percentage of the non-electrical failure rate.
3) System-level models should be sufficiently complex to reflect impacts of operating through different mission phases and with different levels of resilience. In particular:
    a. Models must include even short mission phases where system criticality does not permit NDSEE repair. NDSEE rates usually exceed DSEE rates by orders of magnitude, so such phases can significantly increase mission failure probability.
    b. Models must include the reduced reliability resulting from one or more units in a redundant element going offline, whether permanently due to an irreparable mode or temporarily to repair a reparable mode.
    c. DSEE and other irreparable modes accumulate over the mission, increasing failure rates as the mission progresses.
    d. It is important that simulations reflect the full duration of the mission. Not only can DSEE accumulate over time, but even if all SEE modes are recoverable and the probability of an outage occurring in a single repair time is small, the probability of an outage occurring during the mission may not be negligible if the mission is long enough.
4) If system redundancy serves multiple purposes, all of these purposes must be included in the system models, along with their interferences with each other.
    a. Example: A three-unit element can be used to ensure availability as well as to correct errors that occur within the units by voting. The availability usage has 3:1 redundancy, while voting requires all three units to be functional and will be lost with the first unit failure (that is, no redundancy).
    b. Example: Often, recovery from a reparable SEE may require the entire system to be taken offline for repair and resynchronization, thereby impacting availability.

7.2.2 SEE Testing and Analysis

The following guidelines for SEE testing and analysis are suggested to make best use of system-level modeling results:

1) Use results of system-level reliability and availability assessments to guide SEE test and analysis efforts.
2) Bound the unit and system failure rates using available data to determine whether system SEE rates could affect failure rates unacceptably. Data sources should be prioritized as follows:
    a. Historical heavy-ion test data with suitable margin applied to rates (e.g., >2x for NDSEE, and >5x for DSEE).
    b. Heritage mission data can bound system failure rates if heritage environment bounds that of a proposed mission. Otherwise, nonlinear dependence of system failure rates on unit failure rates preclude use of heritage data.
    c. Historical proton SEE test data can bound system failure rates, provided the mission is short and DSEEs are not a significant concern with conservative analysis/margins.
    d. Data for similar and/or worst-case parts with conservative analysis/margins.
        i. Example: Although most parts have single-event latchup (SEL) rates in the ISS orbit $<10^{-4}$ SEL per day, several parts exhibit rates ~0.01 SEL per day.
3) Use testing and analysis approaches that are consistent with the program's risk position and risk factors.
    a. Proton testing may be acceptable if the mission is short (i.e., hours to days), failure-tolerant, and has easily modeled system responses.
    b. Heavy-ion testing is likely required for selected parts if a mission has low failure tolerance (e.g., Class A or B), is longer than a few days, features complicated systems, and/or makes heavy use of technologies susceptible to DSEE.
    c. Risk factors that exacerbate risk and may increase the need for heavy-ion testing include:
        i. Increasing use of SOTA, COTS, or other technologies with unknown SEE susceptibilities.
        ii. Increasing radiation environment severity.
        iii. Increasing application criticality.
        iv. Increasing mission duration.
4) Prioritize testing based on system-level simulation results and risk, ranking, and the expected benefit from the test.
    a. Identify critical parts, especially those used in systems that would affect multiple other systems or services.

b. Identify parts in heavy usage (e.g., used in >10 to 15% of functions), especially in critical applications.

c. Assess the relative complexity of redundant units/elements as indicated by the number of functions/services the unit provides, and part count (especially parts susceptible to DSEE). All other things being equal, a complex unit will likely have a higher failure rate, thereby driving the system failure rate.

d. Develop a metric for prioritizing heavy-ion testing according to its potential risk reduction. The metric may reflect the criticality of the application, the number of applications, and the relative complexity of the units where it is used. For example, the metric could be a weighted sum over all parts in the system, with the weights reflecting the part criticality and relative unit complexity.

5) To minimize disruption to the design process, develop work-around or redesign strategies for use if one or more of the parts selected for test exhibits unacceptable SEE performance.

8.0 Other Deliverables

No unique hardware, software, or data packages, outside those contained in this report, were disseminated to other parties outside this assessment.

9.0 Lessons Learned

No applicable lessons learned were identified for entry into the NASA Lessons Learned Information System.

10.0 Definition of Terms

Availability	Ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming required external resources are provided [IEC 60050-191- 02-05] *(NESC Team Note: does include repair cycles).* Where reliability is specified in MTBF and maintainability in MTTR, availability equates to = MTBF / (MTBF + MTTR).
DSEE	Destructive SEE includes all permanently destructive modes as well as nondestructive modes that cannot be repaired by the system whereby the system loses its function.
Element	An ensemble of multiple redundant units, which can perform its required task as long as the required number of units are operational.
Non-reparable SEE	Includes all destructive modes as well as nondestructive modes that cannot be repaired by the system.
NDSEE	Nondestructive SEE or Reparable SEE: A reparable mode is a nondestructive SEE from which the system can restore normal operation after a nominal repair time.

Reliability	Probability that an item can perform a required function under given conditions for a given time interval [IEC 60050–191-12-01] *(NESC Team Note: does not include repair cycles).*
Reparable SEE	NDSEE from which the system can restore normal operation after a nominal repair time.
Resilience	The intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions. [Hollnagel, Erik; Resilience Engineering in Practice, 2010]
SEB	Single-Event Burnout—a potentially destructive SEE mode affecting a variety of transistor technologies.
SEDR	Single-Event Dielectric Rupture—a destructive SEE mode in which an ion causes dielectrics in a semiconductor device to fail.
SEGR	Single-Event Gate Rupture—a destructive SEE mode affecting MOSFETs and related technologies.
SEE	Single-Event Effect—Occurs with a variety of consequences, ranging from a momentary disturbance, data corruption or loss of functionality (NDSEE) to catastrophic failure (DSEE).
SEFI	Single-Event Functional Interrupt—a temporary or permanent-but-recoverable interruption in the normal functionality of a microelectronic device.
SEL	Single-Event Latchup, a potentially destructive, regenerative, parasitic failure mode affecting complementary metal-oxide-semiconductor technologies.
SET	Single-Event Transient—a brief disturbance to the output of a semiconductor device.
SEU	Single-Event Upset—a permanent-but-correctable corruption of one or more bits of data in a semiconductor device with bistable (0 or 1) storage cells.
Stuck Bit	Permanent and uncorrectable loss of functionality of a bit in a memory device; although uncorrectable, stuck bits do sometimes repair themselves (anneal).
Survivability	A property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance. [Federal Standard 1037C Glossary of Telecommunication Terms] *(NESC Team Note: for space missions, the system must survive the expanded environment termed "survival temperature limits," launch when launched in the "off" state, and when configured "off" as a cold spare or an on orbit spare.)*
Unit	A box or other hardware designed to perform a designated task as part of a subsystem or system.

11.0 Acronyms List

COTS	Commercial-Off-The-Shelf
DSEE	Destructive SEE
EDAC	Error Detection and Correction
EDL	Entry, Descent, and Landing
EEE	Electrical, Electronic and Electromechanical
FDIR	Fault Detection Isolation and Recovery
FPGA	Field-Programmable Gate Array
ISS	International Space Station
MEAL	Mission, Environment, Application, and Lifetime
MOSFET	Metal-Oxide-Semiconductor Field Effect Transistor
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NDSEE	Nondestructive SEE
NESC	NASA Engineering and Safety Center
PRA	Probabilistic Risk Assessment
RAM	Random Access Memory
RBD	Reliability Block Diagram
ROM	Read Only Memory
SCP	Self-Checking Pair
SEDR	Single-Event Dielectric Rupture
SEE	Single Event Effect
SEFI	Single-Event Functional Interrupt
SEGR	Single-Event Gate Rupture
SET	Single-Event Transient
SEU	Single-Event Upset
SOTA	State-of-the-Art
SWAP	Size, Weight, and Power
TDT	Technical Discipline Team
TMR	Triple-Modular Redundancy

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/12/2019	Technical Memorandum	

4. TITLE AND SUBTITLE
Radiation Single Event Effects (SEE) Impact on Complex Avionics Architecture Reliability

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Hodson, Robert F.; Morgan, Dwayne; Ladbury, Raymond L.; Chen, Yuah; Bay, Michael; Zinchuk, Jeffrey

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
869021.03.07.01.09

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
L-21015 NESC-RP-17-01211

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TM-2019-220269

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category 16 Space Transportation and Safety
Availability: NASA STI Program (757) 864-9658

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The NASA Engineering and Safety Center (NESC) had an urgent need to understand how system-level reliability of an avionics architecture is compromised when portions of the architecture are temporarily unavailable due to single event effects (SEE). The NESC activity parametrically evaluated these SEE impacts on system reliability based on mission duration, upset rate and recovery times for a representative redundant architecture. This document contains the outcome of the NESC assessment.

15. SUBJECT TERMS
Single Event Effect; NASA Engineering and Safety Center; Electrical, Electronic and Electromechanical

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
U	U	U	UU	50	19b. TELEPHONE NUMBER *(Include area code)* (443) 757-5802