JPL D-48258

Jupiter Europa Orbiter (JEO) Radiation Design Guidelines

Prepared by

Ed Shalom
Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, CA 91109

October 14, 2008

Initial Version

Prepared by:

Ed Shalom, Section 3401 — Date: 10-16-08

Concurrence:

Randy Blue, Manager, Sec. 345 — Date: 10-16-08

Gary Bolotin, Manager, Sec. 3401 — Date: 10-16-08

For Pubic Release

Copyright ©2008 by the California Institute of Technology
Government Sponsorship Acknowledged

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

DOCUMENT CHANGE LOG

DATE	PAGES AFFECTED	CHANGES/ NOTES	VERSION/ REVISION
10/14/2008	All	Initial Version	Initial Version

TABLE OF CONTENTS

1.0 SCOPE 1
1.1 Level 1
1.2 Focus on Improvements vs. Existing Practices & Documents 2
1.3 Introduction and Motivation for Guidelines 2
1.3.1 Electronic Lifetime as a Consumable 2
1.3.2 Example of Excessive Conservatism: WCA & Shielding 3
1.3.3 WCA Improvements to be Addressed Separately 4
1.3.4 Compounding Effects of Conservatism & Need for Modification 4
1.4 Providing Guidelines and Tools 4
1.5 Systems Perspective 5
1.5.1 Emphasis on System Engineering 5
1.5.2 JPL Design Principles (DP) 5
1.5.3 EO NonConformance to JPL Design Principles 6
1.5.4 Exceeding the Requirements of JPL Design Principles 6
2.0 REFERENCE DOCUMENTS & EXISTING PRACTICE 6
2.1 Generic JPL HW Development Process Documents 6
2.2 Generic JPL & NASA SW Development Process Documents 7
2.3 JPL Project Life Cycle & Project Documents 7
2.4 System Engineering Guidelines for Avionics Subsystems 8
3.0 CAPTURING REQUIREMENTS 8
3.1 Flow down Requirements: functional & fault protection 9
3.2 Self-Imposed requirements 9
3.3 Verification and Validation (V&V) 9
3.3.1 Increased Emphasis on V&V 9
3.3.2 Linking V&V Between HW & SW Development Levels 10
4.0 DEVELOPING A ROBUST FUNCTIONAL ARCHITECTURE 10
4.1 Inheritance 10
4.2 Inheritance Reviews 11
4.3 Hardware vs. Software Trade 11
4.4 Modularity 11
4.5 Commonality 12
4.6 Model Based Engineering (MBE) 12
4.7 Anticipate Sim & Support Equipment (SSE) Requirements 12
4.8 Power-On vs. Power Off States 13
4.9 FPGA & ASIC Issues 13
4.9.1 Importance of Test Coverage for ASICs 14
4.9.2 ASIC Test Coverage Tools and Techniques 14
4.9.3 IP vs. Custom Code for FPGAs & ASICS 14
5.0 IMPLEMENTING A FAULT TOLERANT SYSTEM DESIGN 15
5.1 Higher Degree of Importance of Fault Tolerance and Fault Protection 15
5.1.1 Development of FP in Parallel with System Architecture 15
5.2 Fault Protection: Fault Containment Regions 15
5.3 Beyond block redundancy 15
6.0 HW IMPLEMENTATION 15
6.1 Subsystem Specific HW Considerations 16

6.1.1 C &DH Subsystem Specific Considerations 16
6.1.2 The NEXUS Bus Option 16
6.1.3 Power Subsystem Specific Considerations..... 16
6.1.4 Telecom Specific Considerations..... 18
6.2 Generic HW Issues 18
6.2.1 Parts & Materials 18
6.2.2 Use of the Approved Parts and Materials List (APML)..... 18
6.2.3 Identification of NSPARs and Waivers..... 19
6.2.4 Early & Close Coordination with Mission Assurance 20
6.2.5 Arrangements for Special Radiation Tests 20
6.2.6 FPGAs and ASICs: rad hardness, cost, lead times 20
6.3 Generic Subsystem Considerations 21
6.3.1 Radiation Level Monitoring 21
7.0 SW IMPLEMENTATION CONSIDERATIONS..... 21
7.1 SW Must Anticipate a More Complex Set of Behavioral Modes 22
7.2 Additional Diligence in Adhering to SW Process 22
7.3 Extra Emphasis on Ground Systems and SW..... 22
8.0 SHIELDING..... 23
8.1 Radiation Design Factor (RDF)..... 23
8.2 Interpreting Data from Radiation and Shielding Analyses 23
8.2.1 Dose Depth Curves 23
8.3 Shielding Techniques..... 23
8.3.1 Previous JPL Shielding Experience 23
8.3.2 Commonality of Shielding Techniques..... 23
8.3.3 Part Level Shield by Vendor: e.g., Rad-Pak..... 24
8.3.4 Part Level by Electronic Packaging: “Spot Shields” 24
8.3.5 Board Level: e.g., a “Clamshell” for NVM Slice 25
8.3.6 Box Level Shields 25
8.4 Using Electronic Packaging as a S/C Structure Component..... 25
9.0 ELECTRONIC PACKAGING: BOARD AND BOX..... 26
9.1 Packaging Approach 26
9.1.1 Traditional..... 26
9.1.2 Micro-Packaging: Chip-On-Board, etc. 26
9.2 Thermal Constraints & Control Context..... 28
9.2.1 Higher Investment in Thermal Modeling & Control 28
9.2.2 Grounding of Conductive Surfaces..... 28
10.0 Materials Issues 29
10.1 Degradation due to Ionizing Radiation (VG Canopus example)..... 29

Link Table..... 299

Additional Resources for Reliability Engineering 30

Acronym List 33

1.0 SCOPE

The scope of this document is to provide guidelines and recommendations to support the design of space avionics in a high radiation environment, such as would be encountered in a Jupiter Europa Orbiter (JEO) mission. It is targeted at the major locations of S/C flight electronics: in the engineering subsystems C&DH, Power, and Telecom, as well as in the science payload.

While the primary focus is on avionics HW, there are a number of areas in which the design of HW design for radiation cannot be effectively decoupled from the SW design. These areas include such topics as systems architecture, fault tolerant design and fault protection implementation, and so on. As appropriate, the interactions between HW and SW would be addressed, and guidelines for the SW component would also be provided.

To a large extent, the guidelines are generic; in cases where there is a particular focus upon a specific area, it shall be identified.

1.1 Level

In general, the intent of these guidelines is to address Requirements Level 4 (Subsystem) and below. However, there are cases where it is appropriate to drive requirements at higher levels.

As a concrete example, it is often the case that during a project life cycle that governing documents that address mission assurance, environmental requirements, and fault protection, tend to be formally released later in the development cycle than preferable.

The late release dates are compounded by a tendency for developers to not carefully scrutinize these documents when they are released. On conventional projects, while this oversight could result in unnecessary waivers or even redesign, the cost of this disconnect is not extremely high. However, when dealing with harsh environmental conditions that implementers are not familiar with, the cost of this disconnect could be severe.

In light of this, this document emphasizes the vital necessity for implementers to pay close attention to the subject class of documents very early in the project life cycle. However, this guideline would be useless if the documents in question are not generated and signed off early on.

Given this reasoning, it is imperative that project planners ensure that work on these documents is fully funded early in the project life cycle. As such, to ensure that this happens, it is deemed appropriate to try to drive requirements upwards in this document. While it is true that this may result in double coverage on such topics, this is preferable to taking the chance they would be overlooked.

1.2 Focus on Improvements vs. Existing Practices & Documents

There is much existing documentation on design practices and processes for both HW and SW that govern development at JPL, other NASA centers, NASA, the military, and the commercial sector. It is not within the scope of this document to cover these existing practices, or even to reference them all.

The primary focus of this document is the focus on suggested improvements to the existing state that are needed to address high radiation environments. However, in order to provide some context for these guidelines, this document does include references to existing process documents, in particular major processes followed at JPL.

1.3 Introduction and Motivation for Guidelines

The traditional methods for designing and verifying spacecraft electronics subsystems leads to a highly conservative system design. This commonly results from two fundamental sources.

The first is that previous projects have had the luxury of essentially not having to address the intrinsic lifetime of parts, which is typically represented as a “bathtub” shaped curve. Previous practice focused on parts burn-in and operating hours prior to launch as a means of weeding out “infant mortality”: once this was accomplished, to a large extent the other “wall” of the bathtub was not addressed, since it was presumed to be far beyond a typical mission life. This assumption has been borne out by numerous electronic assemblies, in which the absence of a latent flaw and/or misapplication, space electronics have operated for decades.

The second fundamental area, aside from part lifetime, is a result of the compound effect of applying worst case conservative assumptions at every level, and allocating margins at each level as a contingency.

These two areas are described in additional detail below.

1.3.1 Electronic Lifetime as a Consumable

In order to maximize the useful lifetime of electronic components in a high radiation environment, a change in mind-set is required. For typical interplanetary S/C, the available lifetime of the electronics far exceeded that of typical in-flight consumables, such as propellant or battery life. As such, absent catastrophic failure of electronic systems, the duration of space missions could potentially far exceed their design limits, subject to the depletion of non-electronic resources.

While it is plausible that S/C and or satellites have failed due to latent defects and/or misapplication of electronic components (example: excessive temperature and current results in electro-migration and part failure) , there does not appear to be any evidence that any JPL space mission (or even, any space mission) was lost because the electronic

parts did not have the intrinsic capability for sustained operation. Missions such as Voyager and MER demonstrate this.

This conclusion is supported by an IOM written by N. Taylor of JPL (IOM 5131-05-112), which states that (the boldface has been added here for emphasis):

> Failure data from JPL missions Viking I and II, Voyager I and II, Magellan, Galileo, and Cassini was used to determine the JPL in-flight part failure rate. The failure data had been previously analyzed and an overall JPL in-flight part failure rate was found to be **0.398 FITs/part**, where 1.0 FIT = 1 failure/10^9 operating hours. This was considered to be the "**JPL Failure Rate**." JPL failure rate information was summarized in Reference 1. A similar approach was used to determine failure rates for parts based only on the **Galileo** mission and only on the **Cassini** mission (up to August 2005). The failure rates derived for those missions are **0.0956 FITs/part** and **0.156 FITs/part**, respectively

Since the FIT rate (failure rate in 10**9 hours) per part for GLL and Cassini were in the regime of 1/10 FIT, and the overall JPL average for flagship missions was about 4/10 FIT, and the lowest levels in industry are on the order 10's of FITs, the record for JPL flagship missions is quite impressive.

When subject to high radiation dosage, the situation changes in a basic way. By necessity, the capability of the electronic parts to tolerate radiation could become the pacing item in determining the nature and duration of the mission. In this manner, the lifetime of electronic components for a JEO mission becomes a consumable, comparable in many ways to consumables such as propellant and battery cycles in previous missions: even though many electronic parts may degrade gracefully under radiation, rather than failing in a catastrophic manner, the design lifetime for JEO HW is expected to be such that after several design lifetimes, the graceful degradation would reach the point of dysfunctionality.

1.3.2 Example of Excessive Conservatism: WCA & Shielding

As an example of excessive conservatism, in the JPL electronics design process, a parts data base is normally constructed that attempts to capture the ranges for all relevant parts parameters (i.e., radiation, power supply variation, end-of-life, and part-to-part variation) for each component. Very often, an additional safety margin is levied on these part parameters. A Radiation Design Factor (RDF) of 2 is typically applied; for example, if the expected radiation environment is 1 Mrad under 100 mils AL, parts would be required to have a tolerance of 2 Mrads under 100 mils AL.

A WCA using extreme value analysis (EVA) is then conducted using these parts parameters, in which every part is assumed to be at the worst possible combination of it's range and thermal environment, with the requirement that the circuit still function. Typically, parts on the same board are assumed to be simultaneously be at PWB (Printed

Wiring Board) temperature extremes if it drives the worst-case scenario, even if it is virtually impossible that this occur.

In the event that the initial circuit does meet the WCA, for example, due to radiation effects, one approach typically taken is to provide spot shielding for the component. However, in designing the spot shield, the packaging engineer is usually required to meet a RDF of 3. Using the example above of an environmental exposure of 1 Mrad, a part that does not have the required capability of 2 Mrad must be shielded so that it could tolerate an exposure to 3 Mrad.

1.3.3 WCA Improvements to be Addressed Separately

An intrinsic part of the traditional flight electronics design process is reliability analyses, in particular Worst Case Analysis (WCA). Improvements in WCA methodology have the potential to measurably improve the confidence level in the performance of electronic systems in high radiation environments.

An effort to make improvements in this methodology, especially as it pertains to high radiation, and confirm the improvements via both test and analysis, is now underway at JPL. When the guidelines for the improved WCA methodology become available, they shall be referenced in future versions of this document. It should be noted that the WCA guidelines are expected to be provided as a supplement to JPL's Reliability Analyses for Flight Hardware in Design (D-5703), rather than supplanting it.

1.3.4 Compounding Effects of Conservatism & Need for Modification

As such, due to a compounding effect of conservation at several levels, a traditional flight system and electronics subsystem design would contain excessive margins that limit resources available for mission science, and in fact may lead to the conclusion that the mission cannot be flown.

A JEO Mission would require innovative design techniques and methods to demonstrate the ability of flight engineering subsystems to operate in the Jovian radiation environment for an acceptable mission lifetime. As pointed above, this development approach could free resources that could be employed by instrument developers.

1.4 Providing Guidelines and Tools

However, in order that instrument developers could benefit from these extra resources, they would require more insight in how to take advantage of them. As such, guidelines, tools, and circuit examples are required.

While it is not expected that instrument developers would follow the practices of the engineering subsystems, previous approaches that just constrained the parts in the instruments and required interface FMECAs are not expected to be adequate for the Europa Explorer Mission. Clarification on how Mission Assurance requirements, such as reliability analyses, may be expanded or altered for a JEO mission is expected after a JPL on-going effort to review these processes is concluded.

In developing the guidelines in this document, it is recognized that it is not useful or practical to repeat all of the processes and lessons learned regarding the implementation of space electronics. On the other hand, in an intense radiation environment, some of these traditional processes require a much higher level of scrutiny and sensitivity. As such, they are included herein, along with content that is unique to this application.

1.5 Systems Perspective

Even when addressing applications such as a single circuit card, it is useful to approach it's implementation as that of a system. While it is useful for organizational purposes to refer to a hierarchy of sub-systems, assemblies, sub-assemblies, and so forth, from a conceptual viewpoint it is logical to consider each level to be a system unto itself. As such, the process of implementing systems applies in a very similar manner to all levels in the traditional hierarchy.

In particular, in the hostile environment of high radiation, it is incumbent upon each level to be aware of the challenges posed by this environment, and the mitigations available, to a much greater degree. In addition, each level should take the initiative to understand interactions at both higher and lower levels in terms of not only performance, but in particular with regard to architecture, robustness, failure modes, fault protection, and so on. This awareness should not be provided solely by "system engineers", who may not be aware of the nuances of these interactions.

As a simple example, as a rule, the mechanical configuration of traditional S/C almost never took into account radiation effects. By contrast, it is expected that a very conscious and rigorous approach would be taken to take advantage of transport analysis (in which various S/C components could provide shielding for others) in the mechanical design of a JEO S/C. In the past, this was done as the exception, rather than the rule.

Based upon this perspective, it is anticipated that the guidelines in this document would be relevant for both small and large systems: e.g., the discussion on architecture and modularity should apply whether the "system" is an ASIC or a subsystem.

1.5.1 Emphasis on System Engineering

It was recommended above that implementers not rely upon system engineering to find gaps and architectural flaws in the system design, but this should not be understood at diminishing the importance of Systems Engineering on a JEO mission.

To the contrary, systems engineering on JEO would require systems engineers with great experience and knowledge, and in addition, those who could be creative and innovative in addressing the unique qualities of this mission. In particular, a JEO mission should seek system engineers who have had experience with fault-tolerant architectures and fault protection systems.

1.5.2 JPL Design Principles (DP)

One of the key roles that systems engineers typically provide on a project is to monitor and report on margins, such as power, mass, and so on. Based upon experience on many

flight missions, JPL has levied practices and constraints for flight projects, and codified these in a set of design principles: “Design, Verification/Validation & Ops Principles for Flight Systems”, commonly referred to as the “DP”.

1.5.3 JEO NonConformance to JPL Design Principles

In order to provide for the occasional non conformance against the DP, JPL has provided a process for doing so, whereby they could be evaluated by the JPL Project Engineering Office (PEO).

While it is not expected that a JEO mission would require wholesale exceptions to the DP, it is plausible that the unique nature of this mission may have a larger number or such deviations and/or a novel set of them.

In order to address this unchartered territory correctly, systems engineering for a JEO mission must conduct a comprehensive review very early in the project cycle, at all levels, in order to identify potential non-compliances with the DP. These proposed exceptions must be evaluated and assessed at the project level to determine if they are indeed necessary. Those that are deemed necessary must be submitted to the PEO at the earliest opportunity, to either receive approval, or to come up with work-arounds otherwise.

1.5.4 Exceeding the Requirements of JPL Design Principles

It should not be assumed that an JEO mission would only seek relief from the DP; it is very plausible to anticipate that in some cases, the unique qualities of this mission would require that it establish more stringent requirements for itself. For example, the uncertainties of estimating the mass of S/C components and structure are usually well understood, so the contingencies in estimating S/C mass could reasonably be established. Since the process of estimating shielding mass is less understood, besides the need for larger contingency in the estimation process, the project may choose to carry a higher margin at the S/C level than the DP requisite figure for this allocation.

2.0 REFERENCE DOCUMENTS & EXISTING PRACTICE

2.1 Generic JPL HW Development Process Documents

There are generic JPL process documents that constrain the end-to-end process of HW development. Items 1 through 4 in the Links Table in this document reference documents that span the following development phases:

- Develop Hardware Products
- Design Product Systems: Flight Subsystem / Instrument Design
- Integrate, Test, and Calibrate
- Operate Product Systems

2.2 Generic JPL & NASA SW Development Process Documents

There are generic JPL and NASA process documents that constrain the end-to-end process of SW development. Items 7 through 10 in the Links Table in this document reference documents that span the following aspects of SW Development.

- Software Development Standard Processes, Rev. 1
- Software Classification, Rev. 0
- Supporting Assets for the Software Development Standard Processes
- Performing Software Process Tailoring, Rev. 0

A link to a family of NASA SW development documents is also provided in the Link Table.

2.3 JPL Project Life Cycle & Project Documents

In general, all JPL technical disciplines should be cognizant of, and base their planning upon the JPL Project Life Cycle, and the generic set of project documents vs. mission phase that govern their activities and deliverables.

However, for a JEO mission, the timing of these documents may be adjusted vs. the standard model, so any changes to this development model at the mission and project level must be communicated clearly to all stakeholders. In cases when implementers feel the phasing of these deliverables is not adequate, they should be pro-active in expressing these needs to higher levels. In some cases, it may be possible to address these needs by providing preliminary, working versions of these documents,

Since many personnel are phased into a project at Phase B (Preliminary Design), or later in the Implementation Phases C, D, & E, it is incumbent upon new personnel to review documents from the Formulation Phase in order to ensure they conform to these documents.

Some of the early documents that should be of special interest for a JEO mission are the Mission Success Criteria, the Project Implementation Plan, the SW Quality Plan, and the Risk Management Plan. Naturally, personnel should also be conversant with the results of all major reviews, at all pertinent levels, including requirement reviews, PDR (Preliminary Design Review), CDR (Critical Design Review), ATLO Readiness Review (ARR) and so on. All disciplines in a JEO mission should pay particular attention to the Fault Management design, and all fault monitors and responses that involve their area.

2.4 System Engineering Guidelines for Avionics Subsystems

A good resource for generic guidelines for System Engineering of Avionics Subsystems is provided in training material developed at JPL, which is maintained on-line at Item 5 in the Links Table in this document. These resources should be consulted by those who have process questions in terms of applying this material to a JEO mission. The JPL individuals who present each segment are identified, and should be consulted if clarification or guidance is needed.

This material is broken down into the following segments:

01 Introduction
02 Introduction to SE at JPL
03 Behavioral Competencies of Highly Regarded SEs
04 Architecting
05 Requirements
06 Interfaces
07 Verification and Validation
080 Model-Based Engineering
081 System Modeling Language (SysML)
09 System Engineering Methodology
10 System Engineering Software Considerations
11 Cost Estimating
12 Cost Management
13 Risk Management
14 Resource Management
15 Reviews
16 Support Equipment
17 Avionics Flight Computers
18 Memory Devices
19 Architecture of Different Vendors (FP Perspective)

As noted above, the concept of a “system” could apply to various levels of HW integration; as such, the material above is applicable to circuits, assemblies, and so on.

3.0 CAPTURING REQUIREMENTS

This process needs extra rigor in the JEO application. Carrying extra capability could have a very high cost in this mission, and the rule regarding having a justification for every requirement, supported if possible by a model of operation, is paramount.

On the other hand, gaps or inconsistencies in the requirements tree could be very costly; even if such deficiencies are identified before launch, the effort to make amends could be very costly in technical and programmatic terms.

3.1 Flow down Requirements: functional & fault protection

A very strict adherence to having a complete and accurate representation of flow-down requirements is required. This is particularly the case for adherence to requirements in the Mission Assurance Plan and the Environmental Requirements Document. All developers much in addition pay careful attention to the Parts Program Requirements and the Approved Parts and Material List; they are expected to be quite different that the documents from previous missions. that many have grown accustomed to.

3.2 Self-Imposed requirements

A requirements database, such as DOORS, provides a mechanism to track flow-down requirements from higher levels in a systematic way. However, such databases cannot provide the insight required for the generation of self-imposed requirements. These requirements must be generated for a JEO mission with a high level of scrutiny and peer reviews. They must have a clear rationale, preferably one supported by models and analysis, and must be justified in terms of ensuring that the higher level objectives are met, and that the risk of doing so is minimized. However, since the JEO mission would only be practical if reasonable performance margins are maintained, the tendency to levy self-imposed requirements that exceed this envelope, just because it is believed the capability exists to meet them, must be avoided.

3.3 Verification and Validation (V&V)

As part of a rigorous stipulation of requirements, a Verification and Validation Matrix must be included that explicitly references every requirement in terms of V&V. This matrix would stipulate the technique or techniques that would certify that the requirement has been met. In order that this mapping be complete, there must be some means to reference the actual test procedure step and/or analysis document that documents the V&V process.

Furthermore, beyond the need to establish and maintain a complete and accurate V&V plan, during the process of certifying the deliverables, is to track progress vs. the plan. This must occur at major junctures in the development process. such as CDRs, Ready to Fab Reviews, and delivery reviews (e.g., HRCRs).

3.3.1 Increased Emphasis on V&V

By it's very nature, the high intensity radiation environment in a JEO mission presents a very difficult burden on V&V. It has always been very difficult and impractical to actually verify parts, assemblies, sub-systems, and the entire S/C under high radiation levels. When such testing is conducted, flight radiation-hard parts must be used, and tested destructively.

On previous missions, this problem could be skirted to some extent by embedding very high conservatism in the selection and derating of parts for radiation effects, as well as accepting a high degree of conservatism in reliability analyses, such as Worst Case Analysis.

The attempt being made to reduce excessive conservatism in the above processes for a JEO mission puts a much higher burden on V&V. The fact that degradation due to radiation becomes in many cases the primary driver of lifetime forces us to increase the emphasis on V&V for a JEO mission. While there must be an increased measure of V&V via testing at the parts level, the reliance upon analytical methods of V&V would intensify significantly.

At all levels in the S/C development process, additional budget and schedule must be allocated in order to address these more deeply, and earlier in the development process, than is typical on a flight project.

3.3.2 Linking V&V Between HW & SW Development Levels

In addition to being cognizant of the increased attention that must be paid to V&V at various levels of development, it should be understood that an intrinsic component of this effort must be higher scrutiny to how V&V at lower levels is linked to, and to some extent repeated, at higher levels of integration. System developers should make efforts to periodically review and scrub requirements with a focus on V&V implications to make sure that both areas are in sync in a seamless fashion.

4.0 DEVELOPING A ROBUST FUNCTIONAL ARCHITECTURE

4.1 Inheritance

All too often, the use of inherited HW & SW has proven to be a disappointment: HW and SW components that were assumed could be used “as is”, or that were assumed could be used with “small” modifications and upgrades, could not deliver upon this promise. Flight projects sometimes realized late in the game that they could have developed these products from “scratch” at less cost and budget.

The wariness that should be applied to such proposed HW products must be heightened for a JEO mission, since it is highly unlikely that inherited HW would have been designed and certified for the JEO environment. Attempts to do so after the fact must be highly structured and complete – the failure to take into account a single critical part may doom the entire exercise.

The use on inherited HW and SW may also come at a price: is the architecture of the inherited HW and SW consistent with an operating environment in which the end of the mission is very likely to be dictated by radiation degradation, which has a good chance of being gradual rather than abrupt, and for which a flexible and responsive HW/SW architecture provides an opportunity to extend the mission, even at some reduced capacity ?

As such, the use of inherited products should not only be assessed in terms of meeting requirements posed by the radiation environment, but should be evaluated in terms of having the internal structure to support detailed on-the-ground testing and

characterization, as well as the modularity and visibility to enhance in-flight operability and trouble-shooting.

4.2 Inheritance Reviews

Based upon the above, the results of trade studies regarding the use of inherited products must be intensive, and should be the subject of formal Inheritance Reviews. Prior to conducting such reviews, the suitability of existing checklists for inheritance reviews used for previous projects should be reviewed very carefully to ensure they are adequate for the unique challenges of a JEO mission.

The criteria for such reviews should penetrate beyond just the question of radiation hardness, and address issues such a failure modes and their signatures, presence or absence of graceful degradation, fault protection scenarios, commands and telemetry aspects, both flight and ground SW impacts, and operational issues.

Furthermore, at such reviews, particular attention should be paid not only to the specification for such products, but the V&V techniques used to certify them: were they complete for their original application ? Do they need to be expanded upon for a JEO mission, and what resources and risks are entailed in this expansion ?

4.3 Hardware vs. Software Trade

In architecting a system, it is common to come across functional elements whose requirements could be addressed by either HW, SW, or a combination of the two.

In making decisions regarding functional partitioning for a JEO mission, it is in general more advisable to choose the “SW only” implementation, if one assumes that the flight computer this code would be ported to would be assured to sustain the radiation environment. This preference is dictated by common sense, since it precludes the entire process of certifying a new, radiation-hard circuit.

However, we should recognize that the more complex behavioral possibilities available in SW could come with a price – one must anticipate the overhead required at all levels, up to ATLO, in order to verify and validate the code. SW that fails could be as injurious to a mission as HW that fails, and could also result in catastrophic failure.

As an example, simulations for an FPGA or ASIC show adequate timing margin, acceptable clock skew, etc., but don’t account for degradation of the device parameters under radiation. If operating under a reduced clock frequency is not acceptable, the practical value of the IP (Intellectual Property) would be diminished significantly if it must be “tweaked”.

4.4 Modularity

A strong modular design would enhance the ability to design, simulate, and test functionality both under normal conditions and under an extensive FP (Fault Protection) environment.

In dealing with anomalies, both on the ground and in flight, a modular design would simplify the process of trouble-shooting: it would be easier to isolate the problem, simplifying fault trees, and reducing the test and analysis effort required to converge upon the root cause. For a JEO mission, this is of greater importance than usual. As such, designs should not only be reviewed in terms of meeting requirements, but extra effort should be devoted to finding the simplest and most transparent implementation.

While a JEO mission is designed survive long enough to meet its minimum requirements, and would hopefully operate further, albeit with graceful degradation, a highly modular design improves the likelihood that an extended mission would result, in that it enhances testability, improves the robustness of the fault protection system, and increases the ability of the ground system to react to changes in the S/C operability.

4.5 Commonality

Commonality in the JEO mission application is of even greater benefit than normal – everything new and different we create not only increases the burden on parts acquisition, design, fabrication, and so on, but due to the strong FP content of this mission, V&V become very onerous

For a JEO mission, commonality places a much reduced burden on support activities involved with parts acquisition, structural and thermal analysis, extensive transport analysis and design of unique shielding for electronics, and so on.

4.6 Model Based Engineering (MBE)

Model based engineering is always a valuable asset in developing complex systems, becomes of vital important for an JEO mission. Primarily, this is because the V&V effort for such a mission must of necessity rely upon analytical techniques, which are no better than the models underpinning them.

In order to reap the full benefits of MBE, the use of models should be introduced at the earliest opportunity. All requirements need to have a justification, and the different classes of models provide a traceable basis for such requirements, and a good basis for making adjustments to requirements as the development process proceeds.

In addition, the incorporation of models that could be executed in a complex simulation environment enhances the testability of units that could not be fully exercised otherwise.

4.7 Anticipate Simulation & Support Equipment (SSE) Requirements

By necessity the stipulation of requirements and the selection of an architecture for a JEO mission would be driven by radiation data and analytical models for performance and lifetime. This should be taken in cognizance at the very earliest stages of the design process from the V&V perspective, as part of a “design for test” philosophy.

The requirements for the SSE required for V&V, both hardware and software, should be identified in parallel when levying performance requirements. In fact, given the nature of this mission, it is expected that there would be a larger than typical simulation component in the SSE, which would in many cases require a considerable amount of time and resources.

4.8 Power-On vs. Power Off States

HW implementers should be aware of the fact that there is no hard and fast rule regarding radiation damage as a function of bias state: some components would be relatively immune to TID (Total Ionizing Dose) damage when powered off; some components would actually incur greater damage when in a power up state vs. a power down state. Since most printed circuit cards would have a mixture of such components.

A complex trade – use in extreme situations where we need to take advantage of whether there is a significant difference in radiation damage due to being in either a biased or unbiased state. To exploit this difference, the design must be partitioned in such a way that the components in each separately powered module are grouped appropriately. Naturally, the power and thermal impacts of maintaining “warm spares” needs to be factored into the trade space.

4.9 FPGA & ASIC Issues

The introduction of FPGAs and ASICs into a system architecture requires careful attention to the unique aspects of these components. For example, functional testing alone is not adequate for ASICs; even if the ASIC design is logically correct, an individual component may contain a latent defect that may not become visible during functional testing.

It is possible that such latent defects could be exacerbated by a high radiation environment, so the protection afforded by post-manufacturing tests, such as those discussed below, may become of greater importance for a JEO mission than is normally the case.

Given that the high radiation environment encountered in a JEO mission increases the challenges involved in FPGA and ASIC component selection and design, efforts are underway at JPL to address:

- Component selection: for the current and near-term market, identify acceptable ASICs; for payload applications, identify acceptable FPGAs in terms of their Single Event Upset (SEU) mitigation techniques
- Guidelines designing FPGAs
- Guidelines for Converting existing FPGAs to ASICs
- Guidelines for designing new ASICSs (of special interest since an interim FPGA design is becoming commonplace for complex ASICs)

When the final results of these efforts are published, they will be referenced in future revisions of this document. Since there are some generic FPGA and ASIC issues that planners should be sensitive to, some of the major ones are described below.

4.9.1 Importance of Test Coverage for ASICs

In order to deal with the potential of latent faults that are not uncovered by parametric tests conducted by the ASIC foundry, ASICs should be tested with a set of "test vectors", which could identify "stuck-at" faults. For realistic designs, the fault coverage from these test vectors cannot achieve 100% coverage, so a point design would have to make trades between an acceptable level of fault coverage, and the time and resources required to achieve it.

It should be understood that the confidence level provided by a certain fault coverage percentage is a function of the yield of the manufacturer. For example, if the yield is 80%, and the test coverage is 90%, the "test escapes" would be 2%. An equivalent way to state this is that out of every 100 parts, 20 would be defective, 18 of these 20 would be discarded by the test vectors, and that on the average 2 of 100 parts would have latent defects. If 50 parts are used on a S/C, this implies that the odds are that 1 of the 50 would have a latent defect.

This example illustrates the need for high test coverage. As such, it is of great importance that this issue be identified at the very beginning of the design process, and that the appropriate architectural and design techniques that have been identified in the literature to enhance test coverage be employed.

4.9.2 ASIC Test Coverage Tools and Techniques

There are tools and techniques that could be employed to increase the test coverage for an ASIC design: these include the use of scan paths, Built-In-Self-Test (BIST; of particular benefit in testing embedded circuits such as RAMs); JTAG boundary scan, IDDQ (during execution of test vectors, faults are identified by monitoring supply current Idd) and ATPG (Automatic Test Pattern Generation). In general, ATPG is used to generate the bulk of the test coverage, which is then supplemented with custom vectors.

4.9.3 IP vs. Custom Code for FPGAs & ASICS

In general, the use of off-the-shelf, certified Intellectual Property (IP) content for FPGAs and ASICs instead of custom designs should be preferred, since it is "proven". However, the subject of using IP is very complicated, and there are significant risks to using existing IP. For example, it should be recognized that functionality is being embedded into a different environment than it had been certified with and used within before – the simulations for which this IP was certified may not be applicable to a JEO mission.

5.0 IMPLEMENTING A FAULT TOLERANT SYSTEM DESIGN

5.1 Higher Degree of Importance of Fault Tolerance and Fault Protection

For a JEO mission, the importance of having a fault tolerant design, and implementing an adequate FP system becomes even more pronounced than most other S/C. Due to the extreme environment this mission must endure, the use of heritage HW and SW would surely be diminished – the new content would be very high. Even when heritage HW and/or SW is used, it is likely that the classes of potential faults that my be addressed by FP would grow, and that the number of credible faults within each class would also increase.

Fault protection responses would surely increase in concert, and more complex systems of fault identification and recovery would result, such as fault response trees, tiered fault protection, and so on.

5.1.1 Development of FP in Parallel with System Architecture

While the subject of system architecture vs. fault tolerant design and fault protection are presented in separate portions of this document, in practice they must be considered as concurrent processes. While it is typical to first synthesize a functional architecture, and then consider the implications with regard to robustness, once the process has been initiated, a number of iterations would proceed until a satisfactory configuration is chosen.

5.2 Fault Protection: Fault Containment Regions

In order to properly architect a system and develop a fault protection system, block diagrams should be prepared that clearly identify “fault containment regions”, namely portions of the system from which faults cannot propagate to other regions. This depiction may often lead to revisions of the system design, as it may reveal consequences that are not acceptable.

5.3 Beyond block redundancy

In addition to pursuing the standard trades regarding dual-block redundancy, cross-strapping, triple modular redundancy (TMR), and so on, novel approaches for survival and/or graceful degradation for a JEO environment should be considered. Variations upon these themes should also be reviewed, such as “warm” vs “cold” sparing, especially in terms of acceptable fault identification and response times.

6.0 HW IMPLEMENTATION

Many of the guidelines provided in this document are generic, and do not address a particular S/C subsystem or another. However, there are a handful of “subsystem specific” aspects that merit discussion with reference to subsystem. These are provided below, prior to a discussion of generic topics.

6.1 Subsystem Specific HW Considerations

6.1.1 C &DH Subsystem Specific Considerations

6.1.2 The NEXUS Bus Option

A 3 year JPL R&TD effort, that began in October 2008, is pursuing a "scalable avionics architecture that supports different types of missions and new architectural solutions, such as fractionated spacecraft and multi-platforms/cooperative systems".

It is expected that the NEXUS bus would provide the communications margins and flexibilities to enable simplified spacecraft design and architecture, including science payloads; simplified I&T and ATLO; and a plug-and-play interface to all instruments and subsystems. This work would also result in improved fault tolerance and fine-grained cross-strapping for long life missions in harsh environments.

The Technology Readiness Level (TRL) of the Nexus bus should be high enough at the time that commitments are made for a JEO mission that it could used with low risk. As such, the status of this effort should be evaluated early in the project cycle, with particular focus upon the results of simulation and test, fault protection features, and it's TRL.

6.1.2.1 Anticipating Changes in Threshold Voltages

It is well understood that one of the effects of high levels of TID radiation is a change in threshold voltages in logic devices. To the extent that these effects are in fact characterized to a high degree, the design of circuits and components could sometimes be anticipated by designing in an initial offset, such that the ideal operating condition actually occurs at the middle of the TID exposure.

6.1.3 Power Subsystem Specific Considerations

6.1.3.1 DC/DC Converter losses & Thermal Impact

In estimating power supply losses in DC/DC Convertors, care must be taken not to blindly assume that typical power converter efficiencies for such HW could be maintained in high TID environment. In the case of the off-the-shelf convertors, they are most likely not specified to deal with very high TID radiation – assuming that it is determined that they would survive such an environment, part degradation may increase component power consumption, reducing the efficiency of the unit. For example, for the FET transistors used for switching, the internal resistance of the switch in an "on" state (RDS-on) may increase, dissipating extra power in the part, and contributing to overall losses.

Thermal design of such converters must anticipate this phenomenon as well.

6.1.3.2 Higher Load Demand due to Leakage Current & Thermal Impact

For logic devices as well as transistors, increased exposure to TID radiation normally results in increased leakage current, which in effect increases the demands on DC/DC convertors.

In CMOS logic, which is fundamentally configured using totem pole transistors connected between the supply voltage and ground, the ideal state is for one transistor to be totally "ON" and the other to be totally "OFF". To the extent that the "OFF" transistor exhibits leakage current as a result of TID radiation exposure, it lowers the net resistance of the totem pole pair, increasing the circuit between power and ground.

The impact on FET transistors is somewhat similar. The TID radiation could introduce an offset in the gate voltage threshold, which could result in the transistor being somewhat "ON" when it should be "OFF", with the same impacts as above.

In order to deal with this, the capacity of the DC/DC convertors must be sized to deal with the increased anticipated load.

In this case, the thermal design of the both the load and the converter must be addressed.

6.1.3.3 Monitoring of Increases in Power Consumption and Thermal Effects

It is advisable that extra visibility be provided into power consumption due to increased leakage currents, and the thermal impacts that result, for both on-the-ground development and test, as well as in-flight operation.

Such monitoring should be accurate enough to observe trending, in particular for in-flight monitoring, where such increases may serve as the "canary in the coal mine", giving earlier indications of degradation.

Such circuits need to be relatively immune from the intense radiation themselves, or they could hardly be used for this purpose.

It is recommended that early Phase A and B project funding be directed towards developing such circuits, so they may be used in multiple applications throughout the S/C.

In developing such circuits to measure supply and load currents, it should be recognized that very high precision is not required, but very high precision in identifying the range of values is sufficient: for example, a circuit that reports with high precision that a current is between 0.5A and 0.6A, 0.6A and 0.7A, and so on, may be acceptable, even if there is no knowledge about the specific values between the boundaries. This concept is analogous

to the “idiot” lights for engine temperature in some automobiles, which do not provide a continuous analog gauge, but only an indication that a critical threshold has been reached.

Finally, in order for such monitoring systems to be useful, the expected power consumption levels for S/C HW should be both analyzed and measured, and the nominal power consumption level as well as the min and max be determined at the appropriate levels in the HW hierarchy. In order to support this visibility, the overall avionics architecture, as well as the partitioning of this architecture into discrete functional and physical units, should be done in such a way as to make power supply consumption very closely determined and predictable by S/C state.

6.1.4 Telecom Specific Considerations

Based upon discussions with JPL Telecom personnel, the methods used to analytically confirm worst-case operation differ from those used in the C&DH and Power subsystems. This is a reflection of the uniqueness of telecom HW in terms of its composition, life cycle and development approaches in the telecom subsystem.

For example, telecom units tend to become standardized and used in multiple applications, so that one could often rely upon heritage: the telecom HW used for MSL could piggy-back to a large extent upon the HW used for MRO. In addition, telecom HW involves a mixture of mechanical HW, such as waveguides, and specialized analog signal processing components, that lends itself more to empirical testing, such as voltage and temperature margin tests, rather than a purely analytical approach.

In addition, the telecom subsystem often employs GaS (Gallium Arsenide) components, which could be considered as TID immune for all practical purposes.

Given the unique nature of telecom HW, the tools used for simulation and modeling may also differ from those used in other S/C subsystems. These tools may require upgrades and adaptations in order to address the unique environment of radiation degradation, and special radiation tests, at the part and subassembly level, may also be appropriate in order to reduce risk.

On the other hand, the “hands-on” experience and the benefit of extensive in-flight operation of many telecom circuits bodes well for the WCA refinement process, in that the state-of-the-art of the existing process is well grounded and realistic, providing a sound basis for improving the process, and validating the changes.

6.2 Generic HW Issues

6.2.1 Parts & Materials

6.2.2 Use of the Approved Parts and Materials List (APML)

HW implementers should consult with the APML as early as possible to ensure that the parts and materials on the list are adequate for their needs. It may be possible that parts

and materials could be added to the APML if such requests are made early enough, allowing other potential users to take advantage of using these items in an efficient way.

The proposer, as well as other potential users, would be freed from having to request approval from Mission Assurance for deviations, and would be spared the risk of having a request denied late in the implementation phase.

Even if such a request is denied, making it early gives the proposer time to seek work-arounds and alternatives.

6.2.2.1 Long Lead Time Parts Identification & Budgeting

Designs may be based upon specific rad-hard parts that don't have second sources, are expensive, and which have long lead times. Very early in the project life cycle, in some cases even before System PDR, critical long lead parts should be identified. Even prior to actually incorporating critical, long-lead time parts in electronic schematics, it may be appropriate to seek project funding for the early test and characterization of certain parts.

In anticipation of this for a JEO mission, project planners should ensure that the mission cost profile is adequate to support these requests.

6.2.2.2 Place Price Orders Early and in Quantity

An attempt should be made to place orders for flight parts early, and whether they are actually ordered early in the life cycle or later on, they should be procured in bulk, on an expedited basis, and from a single lot if possible, for several reasons: the cost of the parts may be reduced when buying in quantity, the risk of using the parts would be lower, and if special radiation testing and/or screening tests required, conducting the tests on a single lot would reduce the cost of testing & consume fewer parts, and would allow a uniform set of parameters to be used for the parts parameter data base used in reliability analyses.

6.2.3 Identification of NSPARs and Waivers

It is expected for this mission that in some cases there would be gaps between the Approved Parts & Material List (APML) and the parts required to implement specific functions. When this state exists, non-standard parts should be identified as early as possible, and that NSPARs (Non-Standard Parts Requests) be submitted early to Mission Assurance for preliminary risk assessment.

Furthermore, if it is proposed to utilize parts on the APML beyond their spec limits, Waivers should be prepared as soon as possible, in order to acquire a preliminary risk rating.

In both the cases above, an early recognition that the risk of usage is high could allow the option of considering the usage of other parts, modifying the requirements, and/or modifying the packaging and shielding in order to reduce the risk of the existing application.

6.2.4 Early & Close Coordination with Mission Assurance

A few areas in which close and early coordination with Mission Assurance is advised were described above. The resources to support this interaction should be anticipated in budgets and work agreements by both the implementing parties, and well as by Mission Assurance.

6.2.5 Arrangements for Special Radiation Tests

It is expected that for many parts of interest, radiation data is either not available, or incomplete. For example, TID data may have been acquired at a high dose rate in order to complete the testing more efficiently. As such, the annealing effects that could occur at low dose rate testing would not be apparent.

Radiation experts should be consulted to review the part technology, in particular bipolar vs. CMOS, in order to anticipate whether there is “family data” available on a specific part, and to decide if a special parts testing regimen is required.

JPL has an in-house expertise and capability in conducting both high and low dose rate tests, which are typically preceded by a thermal chamber test to ensure the part is within specification. Depending upon the part type, preparation for the test would require test boards and test SW, and an adequate number of parts must be acquired (on the order of 10 to 20).

As a general rule of thumb, the end-to-end cost for radiation testing at JPL, including the NRE, thermal and radiation testing, and a final report, would be approximately $ 40K.

6.2.6 FPGAs and ASICs: rad hardness, cost, lead times

The trade space in choosing between FPGAs and ASICs is very complex and device dependent. As such, the intent of this section is primarily not to advocate one direction or another, but to stress that this selection should not be taken likely, and to suggest that the all considerations in the table below are taken into account.

Comparison of ASIC vs. FPGA Attributes

Attribute	ASIC	FPGA
Power	Less	More
Performance	Higher	Lower
Schedule	Long Development Cycle (min. 1-2 years)	Short Development Cycle (6 mo. - 1 year)
Cost	Higher non-recurring cost	Lower non-recurring cost
Flexibility	Modifications are costly and slow after fabrication	Easy to modify; RAM-based FPGA can even be modified in flight
Delivery	Need foundry and packaging facility	Just need to program FPGA
Radiation	up to 2 Mrad	Up to 300 Krad

6.3 Generic Subsystem Considerations

6.3.1 Radiation Level Monitoring

Previous JPL S/C that encountered relatively high TID radiation levels, such as Voyager, and Galileo, did not carry any instrumentation to specifically measure such radiation. The degrading effects of radiation were observed indirectly, through changes in the behavior of components. These results helped in understanding radiation levels and their effects in a qualitative way, but not a quantitative one.

Significant levels of resources are expected to be expended in developing subsystems for a JEO missions. It would be of great value for the planned JEO radiation monitoring system to be extensive, so that operations could monitor during flight the actual TID exposure for critical assemblies and components, allowing operational adjustments may be made to mitigate damage.

Furthermore, given the fact that such subsystem hardware is being exposed to radiation levels far in excess of previous missions, there is valuable scientific data to be gleaned regarding the temporal response of subsystems under flight conditions.

Taking the above into account, it is recommended that the subsystem and assembly level designers strongly urge the project to expend funds early in Phase A and Phase B in order to provide an extensive number of simple, inexpensive, and low-power radiation monitors, and make these available to the subsystems and other S/C HW implementers as required.

7.0 SW IMPLEMENTATION CONSIDERATIONS

SW Engineering is both an art and a science, and it beyond the scope of the document to actually review the state of this discipline. It is appropriate to stress that the great importance that is rightfully paid to this area needs even greater emphasis for a JEO mission.

7.1 SW Must Anticipate a More Complex Set of Behavioral Modes

This need is based upon the fundamental reason that a JEO mission must address a complex set of failure modes due to radiation, and that the system SW design must endeavor to interact with the HW in a complex way to respond to these failures. A JEO mission would be unique in that there is a reasonable likelihood that not long after the end of the nominal mission, a number of faults could reasonably be expected to start appearing, and it would fall upon the SW to address as many of these faults as possible, albeit at limited capacity, until there is no choice but to terminate the mission.

Based upon this expected scenario, and the expected set of specific degradation mechanisms, the operating paradigm for SW may need to be extended beyond the polarities of nominal vs. non-nominal operation. For example, assume that there is a well understood degradation of memory cells vs. radiation that is expected to manifest itself towards the end of the mission lifetime. SW developers should consider a broader operating environment in which the measures that could be taken to counteract this are considered an alternate operating mode, rather than a fault protection issue.

Using a crude example, if a long auto trip is planned during which the tire lifetime may be exceeded, monitoring the state of the tires allows one the option to change the operating mode of the vehicle, by driving more slowly, rather than waiting for a tire to fail, and replacing it.

7.2 Additional Diligence in Adhering to SW Process

The decisions and processes followed in implementing flight SW and ground SW for a JEO mission should be extra diligent at all areas and phases of HW/SW development, including architecture, fault tolerance & robustness, testability, flexibility, V&V at all levels, especially the system level (ATLO), and operability vs. operations cost.

7.3 Extra Emphasis on Ground Systems and SW

In a JEO mission, much greater emphasis needs to be placed on the development and verification of ground systems, in particular ground SW products. During operations, ground SW functions as an intrinsic element of an extended fault protection architecture. The ability to quickly and accurately identify not only faults, but trends in S/C operating parameters, is a vital component of this architecture. Adequate schedule and resources must be provided by the project to ensure that this capability is provided and tested in a timely fashion.

8.0 SHIELDING

8.1 Radiation Design Factor (RDF)

JPL mission assurance documents would specify the RDF to be used for electronic parts – this is nominally 2, but may vary on a part by part basis. Designers and reliability analysts should ensure that they are aware of the pertinent RDF to be used in their work.

8.2 Interpreting Data from Radiation and Shielding Analyses

8.2.1 Dose Depth Curves

In interpreting data generated by radiation analysts, such as dose depth curves, care must be taken to ensure that this data is interpreted correctly, since it is sometimes confusing for those who not experts. For a JEO mission, where the consequences of misuse or misunderstanding of this data may be severe, the experts who generate this information should be consulted if there if there is any need for clarification or guidance.

8.3 Shielding Techniques

8.3.1 Previous JPL Shielding Experience

On previous S/C missions that had to deal with significant levels of TID radiation, such as the Galileo mission to Jupiter, the need for radiation shielding was the rule, rather than the exception. The different techniques used to provide shielding were done on a custom basis.

During previous work on the JPL X2000 Project, a number of S/C missions were to be addressed by a common S/C C&DH bus, one of which involved a mission to Europa. Based upon the hardness of the components and boards available at the time, some novel approaches were generated. These included the design of a “vault” in which some of the computer cards were to be housed; in addition, for the Non-Volatile Memory (NVM) card within this valult, which had very low TID tolerance, a “clamshell” shield was designed to provide additional protection.

While it is expected that the approaches taken for a future mission would divert from the designs for GLL and X2000, a survey of these approaches is being undertaken to provide a reference for future designs. A description of these designs, along with lessons learned, is planned to be included in future revisions of this document.

8.3.2 Commonality of Shielding Techniques

As pointed out above, the use of radiation shields has been occasional on JPL missions, and the designs tended to be unique to each particular instance.

On a JEO mission, the use of shielding would be the rule, rather than the exception. As such, it is recommended that resources be provided early in the project life cycle to develop a number of representative shielding designs that could be applied at the part, circuit card, and box level.

These representative designs could be used early on to help implementers come up with reasonable mass and volume estimates for their HW, and could be adjusted later on to meet specific user needs, while avoiding the need for a wide variety of approaches.

8.3.3 Part Level Shield by Vendor: e.g., Rad-Pak

At least one vendor, and perhaps more,could provide a specialized package for commercial components that could mitigate the effects of total dose radiation, so that they could be used for space applications. The components of interest may be products that have already been adapted for this special packaging, or may be contracted for in the case of special devices. The technique described below may be most cost effective in certain applications, so developers should make sure they are conversant with it.

In a nutshell, the approach taken is to place a die on a substrate and sandwich it between sheets of a material such as Kovar. To the extent that such a package has already been developed for another application, at times the only change needed for another application is to adjust the thickness of the shields.

It should be emphasized that much of the use of this technology had been driven by satellite applications rather than deep space missions. In addition, the mitigation effects differ considerably if the radiation environment is electron dominated (e.g., Geo orbits) vs. proton dominated radiation (e.g., Leo orbits): for these orbits, the mitigation for the former case is about an order of magnitude greater than the latter.

The vendor we are aware of for such devices is Maxwell Technologies, who acquired Space Electronics Inc (SEI) in 1999, who had developed this proprietary technology and marketed it under the trade name “RADPAK”. Maxwell currently market these components under the trade name “RAD-PAK”. The inclusion of this information provided by Maxwell below is for reference only, as any particular application with this vendor or any other must be done on a case-by-case basis.

According to Maxwell, RAD-PAK products are being used by over 100 space programs. Examples of their products include EEPROM, SRAM, DRAM, A/DC, and FPGA (up to 50K gates, Latchup Protected).

8.3.4 Part Level by Electronic Packaging: “Spot Shields”

At times, it is most effective to shield an individual part or parts rather than an entire board or subassembly. Such “spot shields” were designed for JPL missions such as Galileo; the existing drawings need to be evaluated with care, since most flight electronics on Galileo utilized “dual-shearplate” packaging, and took advantage of the fact that a metal shearplate was configured under the parts, and contributed to the shielding mitigation provided by the top shield.

JPL techniques for designing spot-shields for radiation are documented in Section 1.3.11, Radiation Shielding” in JPL D-8208, “Electronic Packaging/Cabling Design

and Fabrication", Rev K. This section provides mechanical drawings for shielding of transistor "cans" and flat pack components, and may not be entirely up-to-date with other package types.

The current revision of this document and a packaging specialist should be consulted when considering this approach.

8.3.4.1 Grounding of Spot-Shield Surfaces

Being that spot shields are implemented with metallic materials, the rules regarding the grounding of metallic surfaces must be obeyed.

8.3.5 Board Level: e.g., a "Clamshell" for NVM Slice

An example of a board level shield is provided by the "clamshell" shield developed for the Non-Volatile Memory (NVM) card that was to be utilized as part of JPL's Avionics development, which targeted a previous Jupiter orbiter mission, as well as several others.

This NVM card was a PCI-bus based card provided by SEAKR Engineering, who designed the clamshell.

8.3.6 Box Level Shields

In some cases, the most efficient shielding approach is at the box level; for example, this would apply in the case of a large Solid State Recorder (SSR), which contained a number of cards that all had large numbers of memory components that required shielding.

The application of the material for the radiation shield could be in the form of sheets of a particular material, such a copper-tungsten, over an aluminum chassis. At times, it is appropriate to consider a somewhat thicker radiation shield, and to dispense of the separate chassis. In such cases, the properties of the shield material should be evaluated carefully in terms of structural parameters and the fabrication process.

8.4 Using Electronic Packaging as a S/C Structure Component

JPL has migrated away from a packaging paradigm that was used for flagship missions such as Voyager, Galileo, and Cassini, in which the packaging of flight electronics was accomplished as an intrinsic element of S/C structure. This approach, known as "dual-shear plate packaging", was an integrated, uniform packaging approach, in which the electronic assemblies were utilized as load-bearing components of the S/C structure. For example, in the case of Cassini, "the Electronic Packaging Subsystem (EPS) consisted of the electronics packaging for most of the spacecraft in the form of the 12-bay electronics bus. The bus was made up of bays containing standardized, dual-shear plate electronics modules."

While it is not being suggested here that a JEO S/C revert to this particular approach, the fact that the total aggregate shielding mass that has been estimated for JEO is on the order

of 250 kg (including contingency) should drive us to consider whether a other EPS approaches should be evaluated for JEO. This fresh look may result in an innovative EPS design that looks at the shielding and structure in an integrated fashion, and reduces the combined mass of packaging and structure.

9.0 ELECTRONIC PACKAGING: BOARD AND BOX

The compound effects of shielding due to S/C orientation and structure should be taken into account very early in the design cycle. Transport analysis could assist in determining the actual radiation dosage in a particular S/C location and orientation. For this mission type, it is expected that such analyses would become more the rule rather than the exception.

Implementers of S/C hardware should anticipate that their packaging engineers may need numerous iterations of their packaging design approach in order to obtain the best shielding configuration for individual modules on a case by case basis, and should expect numerous iterations with the S/C level structure and thermal engineers, who would have to make complex trades between competing interests.

In this environment, it is recommended that at the Flight System level that adequate resources would be provided to support these trades, which are likely to require significantly more resources than previous S/C.

9.1 Packaging Approach

9.1.1 Traditional

The traditional JPL approach to packaging design is documented in D-8208, “Spacecraft Electronic Packaging/Cabling Design and Fabrication” which has the benefit of codifying decades of JPL experience in all aspects of electronic packaging and cabling.

The general rules and guidelines in this standard tend to be conservative, as they are oriented towards satisfying a broad range of missions. It is likely that in same cases, HW providers would wish to seek some relief with regard to the requirements of D-8208. In such cases, a packaging expert from JPL’s Section 374, Electronic Packaging and Fabrication Engineering Section, should be consulted.

9.1.2 Micro-Packaging: Chip-On-Board, etc.

Key benefits that could accrue from micro-packing techniques, such as Chip-On-Board (COB) are reductions in mass and volume, and a consequence, reduction in shielding mass. For this mission, these benefits may be such that they enable the implementation of a particular electronics module, or even an entire instrument.

These benefits cannot be acquired without extra budget, schedule, and technical expertise. Some of the key areas that must be addressed for COB packaging are described below.

9.1.3 Die Considerations for COB Packaging

Typically, flight electronics uses packaged parts that have been screened to high reliability requirements. While die could be procured prior to installation in packages, vendors do not typically sell "Known Good Die" (KGD), die which have been screened to the same regimen as packaged parts.

Vendors may agree to contract to provide KGD, or the user may procure the die and have the screening performed by a 3rd party. These 3rd parties should be experienced, and should have the fixtures and software necessary to perform this screening.

Screening at the die level needs to address the issue of how to make connections to the die for testing, and yet not compromise the usage of flight pads. Ideally, a die would have a secondary connection for each pin that could be used for screening.

A simpler approach may be to do burn-in at the assembled board level, building enough units to allow for attrition. However, burn-in only identifies functional failures vs. parametric failures provided by KGD. This may not be as significant an issue for instrument electronics vs. engineering subsystems.

Burn-In at the board level should ensure that the temperature ranges and durations do not compromise the integrity of the board and it's materials. It has the potential to save lots of cost and schedule vs KGD.

9.1.3.1 Passive Component Considerations for COB Packaging

Resistors: Standard SMT (Surface Mount Technology) chip resistors could be procured to high reliability standards and used as in conventional JPL flight electronics.

Capacitors: Using high reliability SMT chip capacitors is challenging for COB usage due to size limitations. In order to conserve board space, the MSL Cold Encoder used smaller commercial capacitors. In this case, for the lots procured, a sampling of parts were tested by the TCRE program (these tested parts did not fly). For flight electronics usage, this approach required a parts Waiver.

Inductors: Inductors with reasonable L values are hard to acquire in reduced form factor.

9.1.3.2 PWB Design and Processes Considerations for COB Packaging

The designer of a PWB that uses Chip-On-Board technology cannot rely upon the Design Rules that are used for packaged parts, such as those contained in JPL's D-8208 Electronic Packaging standard. A set of PWB design rules have been developed at JPL for the Distributed Motor Controller and Cold Encoder, and captured in separate documents. These may ultimately be merged into D-8208 in the future.
If not available, die footprints may need to developed.

Depending upon the thermal environment (range and cycles) that the board must survive, careful thought must be given to wire bonds between the die and the PWB, including the materials used to plate the pads on the board, the material used for the wire bonds, and the wire bonding technique.

9.1.3.3 PWB Assembly Considerations for COB Packaging

The assembly of COB electronics should be carried out in an experienced facility. JPL's hybrid lab has had the capability to assemble very high quality COB assemblies that rival those produced by commercial companies that have very expensive automated capital equipment.

There are a small number of companies that JPL has accepted as having the capability to assemble COB boards – for example, the MSL Cold Encoders were assembled at Stellar Microelectronics in Valencia CA.

Unless the quantity of units to be assembled is large (such as the approximate 120 Cold Encoders assembled for MSL) the cost of using commercial vendors for COB could be prohibitive due to the high NRE costs for automated production.

9.2 Thermal Constraints & Control Context

It is the intent of the JEO mission to carry a uniform and reasonable level of conservatism in design and analysis activities. A large component of meeting this burden is due to the known variation in parts performance vs. temperature. At times, the temperature range that needed to be addressed in design and analysis far exceeded the flight operating temperature range. This approach could be justified for other missions, in which there was plenty of operating margin to begin with, and it was easier to take this approach than to expend the resources necessary to predict the actual flight temperature range with high precision.

9.2.1 Higher Investment in Thermal Modeling & Control

For a JEO mission, there should be an investment in early and comprehensive thermal modeling and design, and well as complete thermal balance tests during S/C thermal vacuum testing to validate the thermal model. In addition, consideration should be given to levying more strict thermal control requirements upon specific assemblies. The benefits of this effort could be significant; if the HW is only required to meet its worst case performance over a limited temperature range, the design margin acquired as a result could be applied to dealing with radiation damage. As such, this improved thermal design and analysis provides a means of extending the capability to tolerate TID radiation.

9.2.2 Grounding of Conductive Surfaces

Very careful attention must be given to the need to ground conductive surfaces in order to prevent charge buildup and discharge during flight. As part of the JEO pre-project activities, guidelines would be developed to focus on these safety measures. Further revisions of this document will explicitly reference these guidelines.

10.0 Materials Issues

10.1 Degradation due to Ionizing Radiation (VG Canopus example)

A good example is a leakage path that could result from radiation decomposing a material and/or via electrostatic discharge from an ungrounded shield was documented in Lessons Learned No. 0384 (Lesson Date: 1995-02-15) in the NASA Engineering Network, submitted by JPL. The details of the Lesson Learned are at the following like, and portions of the text extracted below.

http://www.nasa.gov/offices/oce/llis/0384.html

"Subject: Cone Angle Anomaly in Canopus Star Tracker

Abstract:

An anomaly in the cone angle circuitry of the Voyager Canopus Star Tracker was probably due to a Delrin insulating sleeve decomposing after exposure to Jupiter radiation fields, causing a high resistance path through the Delrin. Ground metal shielding boxes and metal masses on circuit boards, analyze/test materials that could be exposed to ionizing radiation, and maintain spare hardware to enable failure analysis.

Description of Driving Event:

Shortly after Voyager 1 Jupiter encounter, an anomaly occurred in the cone angle circuitry of the Canopus Star Tracker (CST). The cause of the problem was determined to be a base-emitter or collector-emitter leakage in a transistor circuit that drives the cone angle deflection plates. This problem was duplicated in a spare CST.

The most probable cause of the leakage path in the transistor circuitry is believed to be two-fold; 1) a Delrin insulating sleeve decomposed after exposure to Jupiter radiation fields and 2) development of a high resistance path through the Delrin by electrostatic discharge from an ungrounded tungsten radiation shield box.

Lesson(s) Learned:

Charging of internal elements to as high as several hundred volts can occur due to radiation fields.

Exposure to ionizing radiation can degrade spacecraft materials.

Availability of spare hardware is extremely useful in verifying in-flight failure modes.

Recommendation(s):

All metal shielding boxes and metal masses on circuit boards should be grounded even though they are inside equipment housings.

All materials that could be exposed to ionizing radiation should be analyzed/ tested to insure that unacceptable degradation would not occur.

A set of spare hardware should be maintained to enable analysis of in-flight failures and validation of proposed corrective actions."

LINK TABLE

JPL:

1. Develop Hardware Products
http://rules.jpl.nasa.gov/cgi/doc-gw.pl?DocID=57573

2. Design Product Systems: Flight Subsystem / Instrument Design
http://rules.jpl.nasa.gov/cgi/doc-gw.pl?DocID=57396

3. Integrate, Test, and Calibrate
http://rules.jpl.nasa.gov/cgi/doc-gw.pl?DocID=57512

4. Operate Product Systems
http://rules.jpl.nasa.gov/cgi/doc-gw.pl?DocID=57472

5. Avionics Subsystem System Engineering Training
https://bravo-lib.jpl.nasa.gov/docushare/dsweb/View/Collection-82786

6. Division 34 Engineering Practices Manual
http://rules.jpl.nasa.gov/cgi/doc-gw.pl?DocRevID=38704

7. Software Development Standard Processes, Rev. 1
http://software/productLink.cfm?fileID=74352&LinkType=2&CatID=27

8. Software Classification, Rev. 0
http://software/productLink.cfm?fileID=71692&LinkType=2&CatID=27

9. Supporting Assets for the Software Development Standard Processes
http://software/subCategory.cfm?category=27&subcategory=450

10. Performing Software Process Tailoring, Rev. 0
http://software/productLink.cfm?fileID=77552&LinkType=2&CatID=27

NASA

11. NASA SW Standards
http://software/category.cfm?category=14

GSFC:

12. Goddard Space Flight Center, Office of Logic Design
http://klabs.org/DEI/References/design_guidelines/nasa_guidelines/index.htm

MILITARY:

13. Electronic Reliability Design Handbook, MIL-HDBK-338B
www.barringer1.com/mil_files/MIL-HDBK-338.pdf

14. Reliability Prediction of Electronic Equipment
snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-217F-Notice2.pdf

Additional Resources for Reliability Engineering

Sources below from Wikipedia site "Reliability Engineering":

http://en.wikipedia.org/wiki/Reliability_engineering

Texts

Blanchard, Benjamin S. (1992), *Logistics Engineering and Management* (Fourth Ed.), Prentice-Hall, Inc., Englewood Cliffs, New Jersey.

Ebeling, Charles E., (1997), *An Introduction to Reliability and Maintainability Engineering*, McGraw-Hill Companies, Inc., Boston.

Denney, Richard (2005) Succeeding with Use Cases: Working Smart to Deliver Quality. Addison-Wesley Professional Publishing. ISBN . Discusses the use of software reliability engineering in use case driven software development.

Gano, Dean L. (2007), "Apollo Root Cause Analysis" (Third Edition), Apollonian Publications, LLC., Richland, Washington

Kapur, K.C., and Lamberson, L.R., (1977), *Reliability in Engineering Design*, John Wiley & Sons, New York.

Kececioglu, Dimitri, (1991) "Reliability Engineering Handbook", Prentice-Hall, Englewood Cliffs, New Jersey

Leemis, Lawrence, (1995) *Reliability: Probabilistic Models and Statistical Methods*, 1995, Prentice-Hall. ISBN 0-13-720517-1

MacDiarmid, Preston; Morris, Seymour; et al., (1995), *Reliability Toolkit: Commercial Practices Edition*, Reliability Analysis Center and Rome Laboratory, Rome, New York.

Modarres, Mohammad; Kaminskiy, Mark; Krivtsov, Vasiliy (1999), "Reliability Engineering and Risk Analysis: A Practical Guide, CRC Press, ISBN 0-8247-2000-8.

Musa, John (2005) Software Reliability Engineering: More Reliable Software Faster and Cheaper, 2nd. Edition, AuthorHouse. ISBN

Neubeck, Ken (2004) "Practical Reliability Analysis", Prentice Hall, New Jersey

Neufelder, Ann Marie, (1993), *Ensuring Software Reliability*, Marcel Dekker, Inc., New York.

O'Connor, Patrick D. T. (2002), *Practical Reliability Engineering* (Fourth Ed.), John Wiley & Sons, New York.

Shooman, Martin, (1987), *Software Engineering: Design, Reliability, and Management*, McGraw-Hill, New York.

Tobias, Trindade, (1995), *Applied Reliability*, Chapman & Hall/CRC, ISBN 0-442-00469-9

Springer Series in Reliability Engineering

Nelson, Wayne B., (2004), *Accelerated Testing - Statistical Models, Test Plans, and Data Analysis*, John Wiley & Sons, New York, ISBN 0-471-69736-2

US standards

MIL-STD-785, *Reliability Program for Systems and Equipment Development and Production*, U.S. Department of Defense.

MIL-HDBK-217, *Reliability Prediction of Electronic Equipment*, U.S. Department of Defense.

MIL-STD-2173, *Reliability Centered Maintenance Requirements*, U.S. Department of Defense.

MIL-HDBK-338B, *Electronic Reliability Design Handbook*, U.S. Department of Defense.

MIL-STD-1629A, *PROCEDURES FOR PERFORMING A FAILURE MODE, EFFECTS AND CRlTlCALlTY ANALYSIS*

MIL-HDBK-781A, *Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production*, U.S. Department of Defense.

IEEE 1332, *IEEE Standard Reliability Program for the Development and Production of Electronic Systems and Equipment*, Institute of Electrical and Electronics Engineers.

Federal Standard 1037C in support of MIL-STD-188

UK standards

In the UK, there are more up to date standards maintained under the sponsorship of UK MOD as Defence Standards.

The relevant Standards include:

DEF STAN 00-40 Reliability and Maintainability (R&M)

PART 1: Issue 5: Management Responsibilities and Requirements for Programmes and Plans

PART 4: (ARMP-4)Issue 2: Guidance for Writing NATO R&M Requirements Documents

PART 6: Issue 1: IN-SERVICE R & M

PART 7 (ARMP-7) Issue 1: NATO R&M Terminology Applicable to ARMP's

DEF STAN 00-41 : Issue 3: RELIABILITY AND MAINTAINABILITY MOD GUIDE TO PRACTICES AND PROCEDURES

DEF STAN 00-42 RELIABILITY AND MAINTAINABILITY ASSURANCE GUIDES

PART 1: Issue 1: ONE-SHOT DEVICES/SYSTEMS

PART 2: Issue 1: SOFTWARE

PART 3: Issue 2: R&M CASE

PART 4: Issue 1: Testability

PART 5: Issue 1: IN-SERVICE RELIABILITY DEMONSTRATIONS

DEF STAN 00-43 RELIABILITY AND MAINTAINABILITY ASSURANCE ACTIVITY

PART 2: Issue 1: IN-SERVICE MAINTAINABILITY DEMONSTRATIONS

DEF STAN 00-44 RELIABILITY AND MAINTAINABILITY DATA COLLECTION AND CLASSIFICATION

PART 1: Issue 2: MAINTENANCE DATA & DEFECT REPORTING IN THE ROYAL NAVY, THE ARMY AND THE ROYAL AIR FORCE

PART 2: Issue 1: DATA CLASSIFICATION AND INCIDENT SENTENCING - GENERAL

PART 3: Issue 1: INCIDENT SENTENCING - SEA

PART 4: Issue 1: INCIDENT SENTENCING - LAND

DEF STAN 00-45 Issue 1: RELIABILITY CENTERED MAINTENANCE

DEF STAN 00-49 Issue 1: RELIABILITY AND MAINTAINABILITY MOD GUIDE TO TERMINOLOGY DEFINITIONS

ACRONYM LIST

A/DC	Analog to Digital Converter
APML	Approved Parts and Materials List
ARR	ATLO Readiness Review
ASIC	Application Specific Integrated Circuit
ATLO	Assembly, Test, & Launch Operations
ATPG	Automatic Test Pattern Generation
BIST	Built-In Self Test
C&DH	Command and Data Handling
CDR	Critical Design Review
CMOS	Complementary Metal-Oxide Semiconductor
COB	Chip-On-Board
CST	Canopus Star Tracker
DOORS	Requirements Tracking System
DP	(JPL) Design Principles
DRAM	Dynamic Random Access Memory
EEPROM	Electrically Eraseable Programmable Read Only Memory
EPS	Electronic Packaging System
EVA	Extreme Value Analysis
FET	Field Effect Transistor
FIT	Failures in 10^9 operating hours.
FMECA	Failure Mode Effect & Criticality Analysis
FP	Fault Protection
FPGA	Field Programmable Gate Array
GaS	Gallium Arsenide
GLL	Galileo Mission
HRCR	Hardware Requirements Certification Review
HW	Hardware
IDDQ	Faults identified by monitoring ASIC supply current Idd
IP	Intellectual Property
JEO	Jupiter Europe Orbiter mission
JPL	Jet Propulsion Laboratory
JTAG Scan	Joint Test Action Group boundary scan technique
KGD	Known Good Die
MBE	Model-Based Engineering
MER	Mars Exploration Rover mission
MRO	Mars Relay Orbiter Mission
MSL	Mars Science Laboratory Mission
NASA	National Aeronautics & Space Administration
NEXUS	(JPL) Next Bus
NRE	Non-Recurring Engineering
NSPAR	Non-Standard Parts Approval Request
NVM	Non-Volatile Memory
PCI Bus	Peripheral Component Interconnect bus standard

PDR	Preliminary Design Review
PWB	Printed Wiring Board
PEO	(JPL) Project Engineering Office
RDS	Resistance Drain-Source
R&TD	Research & Technology Development
RAM	Random Access Memory
RDF	Radiation Design Factor
S/C	Spacecraft
SEI	Space Electronics Inc.
SMT	Surface Mount Technology
SRAM	Static Random-Access Memory
SSE	Simulation & Support Equipment
SSR	Solid State Recorder
SW	Software
TCRE	Temperature Cycle Resistant Electronics
TID	Total Ionizing Dose Radiation
TMR	Triple Modular Redundancy
TRL	Technology Readiness Level
V&V	Verification & Validation
WCA	Worst Case Analysis
X2000	JPL Advanced Avionics Development Program