On Using Commercial Off-the-Shelf (COTS) Electronic Products in Space

William X. Culpepper, Chief Engineer
Test and Analysis Branch
Avionic Systems Division
NASA's Johnson Space Center

Abstract: NASA's Johnson Space Center (JSC) has utilized COTS products in its programs since the early 1990's. Recently it has become evident that, of all failure modes possible, radiation will probably dominate; sometimes to the point of driving system architecture. It is now imperative that radiation susceptibility be addressed when writing the system requirements. Susceptibility assessment, e.g. testing, must begin early in the design phase to establish performance and continue through the hardware qualification program to prove satisfaction of the original requirements(s). Examples of requirements, testing, and architecture versus failure rate will be given.

1.0 Introduction. The options for developing flight hardware in today's engineering environment have changed dramatically from the Apollo and Shuttle eras. In the past, the then modern technology parts were available with pedigrees for their performance in the ionizing radiation found in orbit. If a particular part in a design did not have the proper pedigree, often there was a part that could be substituted by "similarity". If the similarity option was not available, it was generally practical to find a new part and perform the low energy heavy ion test necessary to establish the susceptibility of the part. In the case of low earth orbit (LEO) for which the manned space program is concerned and on which this paper is centered, most parts were capable of meeting the mission requirements. Those few parts that had unacceptable performance like destructive latch ups were uncovered in the part qualification test regimen. The budgets and development schedules of these programs were compatible with the "part level" assessment technique of that day. Today, budgets are smaller and development schedules shorter. This combination just cannot support the test regimen of examining each individual part by itself in the radiation environment before incorporating it into the design. This is further complicated by the fact that some functions needed on orbit are best satisfied by commercial products; at the part, the board or even the system/box level! Examples of these are GPS receivers, 1553 bus units, DC-DC converters, and even laptop computers. It should be recognized that generally every active electronic part in these products is COTS and has no radiation susceptibility pedigree or similarity to a part that does have a pedigree. The project is then faced with the dilemma of how to qualify a system design for the ionizing radiation environment.

An approach to attacking this dilemma is coming into focus at NASA/JSC. It concentrates on three main areas.

The first area is agreement with the customer that designing and developing the product as "rad hard" is not feasible or affordable except in extreme cases (for example extreme criticality coupled with minimal options for redundancy) or very simple cases. The hurdle here is to come to grips with the fact that there will be a non-zero probability of having an error of some type during the mission.

The second area is centered on deriving requirements that reflect what is felt to really be necessary for the mission to be a success. This can be an interesting exercise in coming to grips with reality. It also can be educational in revealing how politics can influence reality.

The third and last area is to insist that performance be verified by test at the part, board and/or box level. The testing is essential to being successful in today's COTS world. The exact test methodology, or better yet minimum test criteria, plays an important role for this part of the approach and is driven by the mission orbit/trajectory and time duration. For manned LEO missions, high energy proton testing fits nicely.

This paper will explore these three areas in more detail.

2.0 On Accepting Less than "Rad Hard".

For many years the accepted and generally unchallenged requirement for flight at JSC was that every part must pass ionizing radiation tests to an LET (linear energy transfer) of 36 MeV//mg/cm2. Over the years it became accepted by the community that if such a test was passed for every part, the system was "rad hard". Of course such is not true. For example assuming that no latch ups were seen to an LET of 36 does not mean that the threshold for a latch up doesn't exist at 36.1 MeV//mg/cm2. And, in fact if one did exist, then the mean time between failure (MTBF) for such a failure would be on the order of 50 years, assuming a saturated cross section of 1e-2 cm2. And the probability of successfully completing a 10 day Shuttle mission would be approximately 0.999 as calculated by the constant failure rate distribution function of

$$P_S = \text{exponential } (-T/MTBF)$$

Where:
P_S is the probability of completing the mission without failure,
T is the mission time, and
MTBF is 50-years based on an LET of 36 and cross section of 1e-2.

Unfortunately the success probability decreases for the long-term mission like the International Space Station (ISS). With the ISS mission time being 10 years instead of 10 days, the probability of success for the ISS mission drops from 0.999 to approximately 0.82.

Acceptance of less than "rad hard" performance requires that the remaining risk be quantified. Once quantified, this risk can be played into the equation with all other identified risks and a composite probability of success estimated. If this fits in to the overall mission success probability, the radiation assessment criteria meets the project/program needs. This is a much more definitive requirement than the original "test to an LET of 36" criteria.

For the vast majority of hardware flown at JSC, acceptable performance for flight is proven with acceptable performance while in an high energy proton beam (MTBF equal to or greater than 10 years for errors not seen).

3.0 On Realizing Smart Requirements. The crux of successfully utilizing COTS on orbit centers on customer buy-in to the non-radiation hardened product. This buy-in, in actuality, is legally documented in the project/program requirements. It is important that any and all battles be waged and decisively concluded before leaving the requirements stage. If not, the cost of just the ionizing radiation portion of the non-recurring engineering can increase by a factor of 20 to 100. And this doesn't count the effects of lengthening the development schedule or of any redesign impacts.

The Shuttle Cockpit Avionics Upgrades (CAU) is a project currently in development at JSC. It is one of the newest examples of deriving and imposing different requirements to accommodate COTS products in a major program.

3.1 New Radiation Requirements for the Space Shuttle. The National Space Transportation System (NSTS) has the Shuttle or Orbiter as one of the three elements. The other two major elements are the Solid Rocket Boosters (SRB's) and the External Tank (ET). The Orbiter portion of the NSTS is under control of JSC and recently received the "go ahead" to develop upgrades for certain avionic functions in the cockpit. Since JSC has been flying COTS products and relying on them heavily since the mid 1990's, the radiation susceptibility and radiation compatibility questions were well known and a process in place to qualify hardware for flight. It became a matter then of incorporating the proper requirements into the CAU program. However, these requirements must be compatible with the overall NSTS standard, NSTS 07700.

The Orbiter Vehicle End Item (OVEI) Specification, MJ070-0001-1D, is a flow down from NSTS 07700 for the Orbiter vehicle alone. As regards ionizing radiation the OVEI had had the following requirement in force for years:

"3.5.20 Avionics Radiation Requirements. Orbiter avionics designed after February 8, 1993, shall meet the performance and operability requirements while operating within the natural radiation environment, as specified in paragraph 10.1.7.5. All radiation effects, such as, Single Event Upset (SEU), Latchup, and burnout shall be considered."

With the advent of flying COTS parts and products this requirement was proven to be deficient; specifically in the general terminology of "meet the performance and operability requirements while operating in the natural radiation environment". Many interpretations were being used and generally they were an interpretation for convenience and/or profit. For instance, some contractors insisted in one breath that this meant all parts had to be tested to an LET of 36 (which is expensive), but in the second breath used weak if not non-existent similarity analyses to qualify a part as being acceptable in the radiation environment. The end results were that NASA either was spending too

much money and schedule doing heavy ion testing at the part level or NASA, because of inadequate similarity analysis, was sure not of the susceptibility of the products being flown.

After long discussions and heated debate, paragraph 3.5.20 of the OVEI specification was amended to be:

3.5.20 Avionics Radiation Requirements. Orbiter avionics designed after February 8, 1993, shall meet the performance and operability requirements while operating within the natural radiation environment, as specified in paragraph 10.1.7.5. All radiation effects, such as, Single Event Upset (SEU), Latchup, and burnout shall be considered.

For Orbiter avionics designs initiated after January 1, 2000, proof of the ability to meet the performance and operability requirements in the radiation environment shall be established by failure rate estimations at the box or system level. The failure rate estimations shall be based on actual test data although the use of part similarity data shall be allowed as indicated in subsequent paragraphs.

3.5.21 Radiation Testing and Test Data. Radiation testing may be done at the part, board, sub-assembly, and/or system level. Proper test data obtained from other tests may be used where appropriate. The minimum radiation test level required to establish performance and operability levels shall be by exposure of the test article to either

200 MeV (+/- 10 MeV) protons to a fluence of 1E10 protons/cm2, or

heavy ions producing Linear Energy Transfers (LET's) of from 1 MeV//mg/cm2 to 14 MeV//mg/cm2 in appropriate steps of LET to a fluence of 1E6 ions/cm2.

In the former case, the Bendel A data reduction technique is sufficient for estimating the proton cross section curve. In the latter case, the cross section curves must be established from threshold to an LET of 14 MeV//mg/cm2. Radiation induced failure modes not seen during this testing can be expected to have Mean Time Between Failure (MTBF) intervals of ten years or greater.

3.5.20.2 Use of part Similarity Data in Estimating Radiation Susceptibility. The use of similarity shall be defined on a system by system basis. The allowed usage of similarity shall be documented in the system certification plan. When similarity is used to establish the radiation susceptibility of an EEE part by comparison to a 'similar' EEE part that has known radiation characteristics, all elements of the following criteria shall be satisfied:

1. Both EEE parts must be the product of the same approved QPL, QML and/or ISO 9000 manufacturer.
2. Both parts must have been manufactured on the same line.
3. The processing of both parts must have been identical, especially the critical parameters of rate of oxide growth, temperature of the oxide process and final oxide thickness.
4. The two parts must be similar in function and identical in technology

including the same mask design, identical feature size, deposition and doping.
5. The same foundry, off shore or on shore, must have produced both wafers.
Allowable technologies for Radiation Similarity consideration are DMOS, CMOS, VMOS, diffused junction, and alloy junction."
Rationale: Minimum test levels and failure rate estimation requirements are based on independent NASA/JSC research, test, and analysis."

This new requirement does several things:

It establishes that the proof of the ability to meet the performance and operability requirements shall be established at the box or system level. The proof shall be in the form of an estimate of the failure rate (i.e. 1/MTBF).

It requires that this proof be based on test data.

It defines the minimum level of testing that is acceptable. Note that more testing can be done and indeed will be necessary in some cases to prove that the performance and operability requirements have been met.

It establishes the criteria for establishing "similarity" between a part with no radiation pedigree and a part with radiation pedigree. This is not an easy test to pass but it is the criteria recommended by experts in the field.

3.2 Radiation Requirements for the Shuttle Cockpit Avionics Upgrades. The new Orbiter radiation requirements were in place when the CAU program began and resulted in some new and interesting requirements being generated for this upgrade effort. The new is in the sense that the requirements quantitatively addressed the desired probability of success. The interesting is in what actually drove one of the requirements – politics.

Here are the pertinent CAU requirements for performance in the ionizing radiation environment:

Requirement 1: MTBF for Non-destructive Radiation-Induced Events Requiring User Intervention

A single-string of the CDPS hardware shall have a functional interrupt MTBF of 1000 days or greater when evaluated via the methodology of Section 3.5.20 of the OVEI specification.

Rationale: A single string MTBF of 1000 days or greater will support a single functional interrupt every 10 missions for that string. This assumes that the missions are 10 days in duration. Single event effects that are corrected through other means; such as, Error Detection and Correction (EDAC) logic, do not factor into this MTBF calculation. The 1000 day MTBF only applies to uncorrectable errors requiring user intervention. It will be left to the vendor to determine the method in which the hardware will be recovered.

This requirement provides a probability of success of 0.9995 for the worse case dynamic flight of 12 hours for a single string of the CDPS. When it is assumed that there are three operational strings of CDPS hardware, the probability of losing all three strings in the 12 hour period becomes very small [theoretically

(5x10-4)3]. The worse case dynamic flight duration of 12 hours is based on an abort scenario that requires several orbits prior to landing. The 12 hour duration encompasses the time from liftoff to landing.

Erroneous output due to radiation induced events is addressed in the Safety section of this document, 3.3.6.

Requirement 2: Destructive Failures and Non-destructive Latches due to Radiation

The CDPS hardware shall exhibit no destructive failures and non-destructive latches when exposed to a minimum of 200 MeV (+/- 10 MeV) protons to a fluence of 1E10 protons/cm2.

Rationale: Parts that are exposed to the proton test environment and do not demonstrate destructive failure modes and non-destructive latches can be expected to have an MTBF of 10 years or greater if such a failure mode exists. An example of a destructive failure mode would be a destructive failure due to high current or gate rupture.

NASA accepts the risk that some destructive failures and non-destructive latches may occur; however, this probability is deemed small and the risk acceptable. When it is assumed that there are three operational strings of CDPS hardware, the probability of losing all three strings due to this failure mode during a 10 day mission becomes very small [theoretically (2x10-8]. Since the 10 year or greater MTBF associated with these unseen failure modes are of the same order of magnitude as the maintenance calculations and sparing plans for this project, they can be considered with the repair and recovery from non-radiation induced hard failures.

Definition of Functional Interrupt - an ionizing radiation-induced error that requires user intervention for recovery but does not have a latch up or other radiation-induced destructive failure mode as the underlying cause.

The second of the two requirements, that dealing with destructive failure modes, arises from our experience which indicates that it is undesirable to fly any part that can easily be destroyed by a proton event. There may be cases where the part in question is necessary for the mission and in that case the destructive event must be mitigated such that the system can survive the radiation hit and have power recycled to regain operational status. This was done successfully in the early International Space Station (ISS) program for a system called the Early Communications System or ECOM. In general however, heroics such as this should be minimized and that is why the required performance is "latch free". The ECOM situation was that the radiation testing had to be done late in the program evolution and there was no feasible way, financially or schedule-wise, to redesign. Mitigation was the only alternative.

The first requirement regarding the 1000 day MTBF for human intervention is more interesting. Of course one of the failure modes in hardware systems is what we identify as a "functional interrupt" (a concise definition was presented earlier). To the outside observer the functional interrupt presents itself as a condition where the unit is not longer responsive or operating. It

appears to have ceased operating even though it may be drawing no more than the normal amount of power and in some aspects looks as though it is functioning. On the inside the unit has been forced out of its normal operating cycle by a non-destructive event like a bit flip which caused the software to go off program or some other change which halted the normal flow. Recovery from this condition will require human intervention to either initiate a soft reboot in software or to cycle power to bring the unit back up. Functional interrupts are common in hardware systems using COTS products.

The decision to impose a 1000 day MTBF for functional interrupts came from the desire to minimize the need for the astronaut crew to have to service the CAU hardware to correct for the interrupts. The choice of 1000 days was based on what was thought to be an acceptable 'aggravation factor' to the crew work schedule. Of course, testing on the flight hardware design when it is built may find that the 1000 days can't be met. But at least there is an agreed to starting point for the performance and operability requirement.

4.0 Radiation Testing, Test Results and Impacts. In 1995 NASA/JSC was developing a new UHF radio for the Shuttle and ISS crews plus trying to utilize a commercial laptop computer on orbit. The UHF radio became known as the Space to Space Communication System (SSCS) and the laptop, which was the IBM 760XD Thinkpad, became known as the Portable Computer System (PCS). For the SSCS, the radiation testing dilemma was that of not having the budget to individually test with low energy heavy ions the more than 100 different commercial parts in the design. For the laptop the dilemma was that the individual parts could not even be identified as to part type. They were generally IBM proprietary. So part testing with low energy heavy ions was not an option for PCS.

4.1 Radiation Testing with High Energy Protons. The only solution for the SSCS and PCS dilemma was to test with a high energy particle which allows testing at the board or system level. The only high energy particle readily available and affordable is the proton. So high energy proton testing was chosen as the only test avenue that would reveal any data regarding performance of the systems once they were on orbit. The questions that arose were what useful data was gained from the proton test and what was the remaining risk for that portion of the radiation susceptibility that the proton could not explore.

The next 3 years or so were spent trying to model and understand the interaction between a high energy proton and the silicon host medium. Under the leadership of Dr. Pat O'Neill and the late Dr. Gautam Badhwar, NASA/JSC has developed and refined a test philosophy using high energy protons to estimate performance on orbit for both the proton environment and the heavy ion environment. Of equal importance, it also quantifies the remaining risk for failure modes not seen in the proton test. This philosophy has been applied to flight hardware for approximately six years and there have been no surprises from the electronic systems flying on orbit.

The following is a synopsis of this test philosophy:

1. Test with 200 MeV protons to a minimum fluence of 1e10 protons/cm2.
2. Use Bendel A for estimating proton cross section for error rate in the flight orbit.
3. Estimate the on orbit heavy ion error rate contribution from the JSC model.
4. Combine the two rates to estimate the overall error rate.
5. Obtain total dose pedigree during the proton testing.
6. Perform heavy ion tests as needed to define longer term MTBF's as needed.

Note: A 10 year or greater MTBF is expected for failure modes not seen in the proton testing.

For those interested in exploring this further, the pertinent literature reference here is:

"Internuclear Cascade - Evaporation Model for LET Spectra of 200 MeV Protons Used for Parts Testing", O'Neill et al, IEEE Transactions on Nuclear Science, Vol. 45, No. 6, December, 1998, pp. 2467 - 2474.

4.2 Test Results. Some fifty systems have been tested using the proton test approach over the last 6 years. These systems tested range in size from small, single board functional devices like a 1553 bus interface card to a total system like an integrate Global Positioning System/Inertial Navigation System (GPS/INS). All of these systems were tested at the top assembly level using product level or application level test software and approaches so that errors like functional interrupts were seen as close to the level of on orbit use as possible. Conversion of test error rates to expected on orbit error rates becomes much more simple and straightforward.

In more than a few cases, catastrophic failure modes were demonstrated to exist. In every case the failure mode was either designed out or mitigated to an acceptable level of risk. The important point is that, even for off the shelf products, these failure modes were found quickly and inexpensively.

The bottom line, and one which senior management has come to appreciate, is that essentially every system that flies has an MTBF or probability of not completing its mission without some type of failure. This proton testing quantifies these MTBF's and allows project management to accept the risk or take actions to reduce it.

4.3 Impacts. The impacts of testing with high energy protons have been many:

Cost. A 20-20 hindsight case was taken for the SSCS radio system in which a cost comparison was made between making a hypothetical heavy ion test at the part level and the actual cost for the proton test done at the box level. The part level test could not test every part in the box. It tested only some three dozen of the parts felt to be most critical and suspect. The proton test not only tested every active part but also automatically gave a total dose pedigree of 600 Rad(Si). The part level heavy ion test cost roughly $1M which included about 8 man-years of engineering/technician time. The actual proton test cost less than $50K including 0.25 man-years of engineering/technician time. Both estimates include travel and test facility costs.

Awareness. The results of the proton testing has raised awareness that ionizing radiation failure modes are system level problems today. This awareness has become sufficiently dominant so that "rad testing" is becoming a standard part of the hardware "qual program" like thermal/vacuum and vibration. It is being addressed at JSC early in the program evolution.

A Driver of System Architecture. The probability of success equation given earlier in the paper is a powerful tool. Sometimes mighty efforts are made to increase the MTBF of a system and hence improve the probability of success for a mission. There are times when this is not appropriate or efficient. Radiation test results, especially with modern COTS products, are forcing the address of this issue.

A simple example is that of a system built with a 50K hour MTBF. If its use is for a 10 day mission (i.e., the Orbiter), the probability of success is 0.9952. If for any reason that performance was felt to be insufficient, one might try to increase the product MTBF to 100K hours. If after a lot of hard work that MTBF augmentation effort were successful, the probability of mission success would increase from 0.9952 to 0.9976. A paltry return for what probably was a mighty effort. The better approach would have been to make a redundant string for the 50K hour system. The probability of returning from the mission with at least one string working is one minus the probability of losing both strings. With two strings the probability of success goes from 0.9952 to 0.99998.

In today's world of COTS products, it is hard to find a radiation MTBF of 50K hours (5.7 years) at the product level. One should expect radiation failure rates to be a driver in defining overall system architecture.

A Test-Early-Test-Often Philosophy is Needed. A very high quality COTS product used both in civilian aviation and military aviation was selected recently as a candidate product to fill a need in one of JSC's two main manned space flight programs. There is a great deal of data on this product and that data indicated that the overall MTBF of the product in its aviation environment was on the order of 100K hours. This MTBF, coupled with the fact that the product would be used in a triply redundant configuration, seemed much more than adequate from the probability of successfully completing the mission with at least one string still operating. An inexpensive proton test was made on the product and the indicated MTBF from the radiation threat was approximately 168 hours! Even in the triply redundant configuration and with a mission duration of only 10 days, the probability of successfully completing the flight with at least one string still functioning was only about 0.5. While the project is struggling to overcome this set back, at least the bad news was uncovered early in the development program.

5.0 Final Thoughts. Even though very preliminary and incomplete, the latest round of testing modern products has seemed to have a trend toward less tolerance of the products to ionizing radiation. If true, this will make the job of meeting mission success requirements

more difficult. And this will be independent of the type of radiation test done, e.g. proton or heavy ion. It will also further sensitize the design and system architecture to the radiation susceptibility of the electronics. The vigilance to uncover radiation cost drivers must be increased and the awareness of susceptibility addressed as early as the voicing of the very top level system requirements.

While all COTS products are not the same, there are those that are excellent from the standpoint of part selection, design, and manufacture. The use of such COTS in space is one of the enabling features of today's technology. The user, however, must address the radiation issue and settle them. Without COTS products, the manned space flight program payback would be greatly diminished.