

The Intelligent Application Of Quality Management To Smallsat Programs

Brian Cox, Metin Aktik,
MDA
13800 Commerce Parkway, Richmond, British Columbia, Canada V6V 2J3
bcox@mdacorporation, maktik@mdacorporation.com

ABSTRACT: Smallsats are inherently more risky ventures than the traditional space mission. Concept, design, production and integration schedules tend to be much more demanding and the smaller budgets are severely scrutinized. Quality Assurance and Product Assurance are often targeted to keep the final costs in check.

It is a common misconception that quality is difficult to quantify. Costs are often perceived to be large for increasingly shrinking benefits. There have been numerous attempts to establish the true cost of quality by simple breakdowns of process and non-conformance cost and many provide a good estimate of the cost, particularly in organizations with mature quality systems. The cost/benefit ratio or true value of quality is often in dispute; this paper will explore the real benefits to a space missions program of an appropriately tailored quality system.

This paper also argues that one of the major keys to the success of a Smallsat program is the management of risk and the intelligent application of Quality Management principles. As with all engineering projects, normal risk management principles apply to Smallsat missions: risks must be clearly and comprehensively identified, risk mitigation strategies must be formulated and the risks must be managed through the life of the project. Prudent use of Quality Management can be an invaluable tool during the risk management process.

The guiding principal must be to match the quality approach to the requirements; this implies that some requirements such as reliability and spacecraft life may require the usual rigor associated with normal high reliability applications. Other areas of the spacecraft design may claim qualification by heritage and possible delta qualification campaigns.

Reduction of process in Quality Management is the easiest target for project managers but simple reduction must only be undertaken with an assessment of the risks. Challenging the independent decisions of the Material Review Board, for example, may save some dollars in the short term but decisions based on quality criteria always endure. With intense cost and schedule pressures an independent quality voice is essential.

The application of good Quality Management principles also applies to parts selection and there is a tendency to use Commercial Off The Shelf parts because of their enticing cost savings. An assessment of the true costs, quality and reliability of the parts has to be made to assess any inherent risks.

With intelligent application, Quality Management can be a powerful and cost effective tool for risk management on a Smallsat program.

INTRODUCTION

Smallsats And Quality Assurance

In the heady days of the Apollo space program after President Kennedy challenged the United States and NASA to go to the moon and return a man safely to Earth national pride was at stake.¹ At the start of the cold war the space race against the Russians had to be won at any cost. The technologies were so new and the space environment so unknown the overriding theme was that the mission had to succeed. The best and only way forward was to ensure a Quality approach that would guarantee the reliability of the equipment.

Elaborate processes were developed to trace every aspect of the design, procurement, manufacturing, testing, qualification and acceptance of any and all of the parts and units. Checks and balances were put in place so that human error was minimised, analysis techniques developed and implemented to give as much assurance as possible that the final product was safe for man to make the journey to our nearest spatial neighbour. The Russians were to be beaten and nothing was to fail.

The economically affluent 60's and early 70's gave way to a less stable economic climate and a general lack of

public support once the goal had been achieved by Neil Armstrong in 1969.

The Shuttle program continued man's exploration into space although in low earth orbit.

The Faster, Better, Cheaper (FBC) doctrine came about, during the Clinton era when NASA's administrator, Dan Goldin was tasked to cut NASA's budget, considerably.^{2,3}

An easy target was Quality Management. When things were running well Quality was regarded as a huge overhead with very little payback.

The small satellite industry adopted the FBC cliché wholeheartedly; the consequences of mission failure were, after all, far less catastrophic and less visible to the public. There were, and are many successes using the FBC methodology.

There were also numerous failures. A "must read" article by Keith Cowing, written September 15, 2003, provides sufficient food for thought for all that blindly pursue the FBC methodology.⁴

Faster, Better, Cheaper should be the modus operandi for all astute managers, after all that is what managers do. They spend their days optimizing the use of the ever-decreasing resources in order to produce a final product that meets the desired specifications.

What is missing from the Faster, Better, Cheaper doctrine is one very important constraint, namely, do it "intelligently"!

In the 80s and 90's led by the PC revolution and the insatiable demand for personal entertainment, the Japanese showed that enormously high volume; high reliability and highly complex electronics could be produced at extremely low cost.

In the automotive industry air quality concerns led the way for microprocessor controlled emission reduction schemes and electronics were refined that could operate in the much more demanding thermal and vibration environments under the hood of a Toyota (or Buick). Consumer electronics has driven the high tech revolution so parts and processes are now readily available. Space technology can now draw on that experience but it has to be done with intelligence and a pragmatic approach to the risks involved.

In this paper I will attempt to show that Quality Management whether it be Product Assurance or Quality Assurance can be a major tool to add to that

intelligent approach. Throughout the full lifecycle from specification to acceptance and operation the Quality Management function can add a tempering of the project managers enthusiasm to cut budgets and schedule at the cost of final product quality.

RISK

The key to any of this is the management of Risk; so first lets enter into a discussion of what risk is, and how it can be managed in a Smallsat program.⁵

Risk is 'the potential that something will go wrong as a result of one or a series of events'.

It is measured as the combined effect of the probability of occurrence and the assessed consequence given that occurrence. The potential for risk becomes increasingly higher as complexities and new technologies are introduced in the design of systems. Risk in the context of Smallsats is the technical risk of not meeting a requirement or the program risk of not meeting the cost and schedule constraints.

Risk management is the advanced preparation for future events designed to minimize the adverse effects and maximise the positive effects of any event. Risk management is an iterative process that changes throughout the life of a program and is an organized method of identifying and measuring risk and for selecting and developing options for handling that risk.

In the case of Smallsats the greatest risk is the loss of the mission and the subsequent loss of reputation and future business.

Risk management consists of four broad areas:



Figure 1. Risk Management

It is important to be clear on the identification of risks, they must be known problems that have a consequence if they occur, they are not the 'unknown unknowns' that are covered by the usual 15-20% Management Reserve put aside for such events. The risk events must be predictable.

There is also a distinction made between organizational risks and project risks, organizational risks cover such events as legal, insurance, interest and exchange rate risks and are not within the scope of this paper.

This paper is concerned with the project risks associated with designing and building of Smallsats and these include all technical risks, and the risks associated with subcontractors and suppliers.

It is important that risks are well described so that the management can be effective. All risks are stated as a combination of a one Condition and one or more consequences.

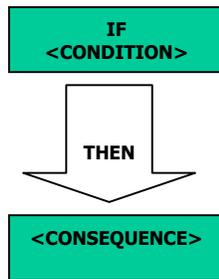


Figure 2. Risk Description

For example:

IF <PCB fails life testing>THEN<redesign is necessary and unit testing will be delayed 15 weeks>

Identification is the most crucial and most difficult stage of the whole management cycle because you are trying to uncover and predict the future. Risk management should be started at the proposal stage of any program.

Based on experience the astute manager/engineer can identify risk areas in each of the proposal, system requirements, Terms and Conditions (T&Cs), The Statement of Work (SOW), Work Breakdown Structure (WBS), supplier and subcontractor relationships, new technology, process, and internal influences (staff, management).

All members of the team should participate in the bottoms-up approach and the key is to write thing down in clear statements and try to go around the review cycle at least twice as there is always something that is missed.

Key techniques for risk identification include brainstorming, Software Engineering Institute (SEI) Taxonomy Based Questionnaire, checklists.^{6,7} All team members must contribute!

The vehicle for the all of the risk management activities is the Risk Management Plan, which may be incorporated in the engineering or management documentation.

Risk assessment and analysis

Once a clear statement of the risks is established the risk assessment and analysis can begin, the purpose of this analysis is to identify the causes of the risk, the effects, the magnitude of the risks and to identify approaches to the risk response.

The analysis determines the probability of the occurrence of event and the consequences of the occurrence. Table 1 shows a Risk Matrix with Severity Categories against Frequency of Occurrence.

Table 1. Risk Matrix

Frequency of Occurrence	Severity Categories			
	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
(A) Probable	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

The important rule is to apply the categories consistently.

Many quantitative models exist to determine the Risk Exposure (RE) but the simplest is

RE = quantitative probability * quantitative impact (in dollars)

On first pass, evaluate RE assuming no mitigation effort

On second pass, think of likely mitigation strategy and adjust RE value.

Risk Planning

The response to a series of risks can be classed as:

- Avoid
- Transfer
- Accept
- Mitigate

As we will see later in this discussion avoidance is key.

AVOID RISKY DESIGN

For Smallsats the primary area of failure is bad design.

Avoidance of risk is the preferred strategy; this means in the early stages of a Smallsat venture it may be possible to challenge the original concept if it eliminates any significant risk.

Transfer of risk is sometimes possible in a customer relationship; this strategy often applies to business rather than technical risks where contractual exclusions and assumptions can reduce the risk to you. But ultimately the risk remains!

Acceptance of a risk is a third possibility; the consequences and probabilities may be so insignificant that the program will just accept them. There are finite risks associated with a launch and insurance may not cover the entire cost. The technology may be new or unproven, qualification inadequate, verification and validation not up to par. The acceptance of risk is normally only an option after careful assessment by independent consultants.

Are you willing to just cross your fingers and hope it doesn't happen?

By far the most acceptable and widely used strategy is to **Mitigate** the risks. This means to reduce the probability and or impact of the threat through active steps.

Any effective mitigation strategy involves:

- Clear action(s)
- Clear resource estimates
- Clear milestones to measure progress
- Continuous tracking/data collection for feeding into the control mechanism i.e. the Risk Status Report
- Clear "triggers" for recognizing risk -> problem transition
- Contingency plan (for dealing with the problem)

On the technical side there are a number of analysis tools that can be used to quantify the risks. These include: Failure analysis including Failure Mode Effect and Criticality Analysis (FMECA), Hazard Analysis and Cause and Effect Analysis. Most of these tools assess the satellite at its End Of Life (EOL).

The tracking and use of Technical Performance Measurements (TPM), which are continually monitored throughout life of the program and critically assessed at major milestone reviews, such as Preliminary Design Review (PDR) and Critical Design Review (CDR) can also track and eventually retire risks.

Testing and the use of environmental testing early in the program can mitigate risks. The use of Structural Qualification Models (SQM), parts testing including Total Ionising Dose (TID) testing, Particle Impact Noise Detection (PIND), Destructive Physical Analysis (DPA) testing, and processes like the Critical Items List (CIL), can all help to mitigate risks.

Risk Control

Risk control meetings should be held monthly and should be attended by the Quality representative and all the risk owners. Each risk is reviewed and all risk attributes (probability, severity, exposure, timeframe, priority, mitigation, trigger, contingency plan) need to be reviewed as well as latest mitigation status.

Control actions that can be implemented include:

- Risk closure
- Continue mitigation
- Change mitigation strategy
- Execute contingency plan (ouch!)

And always remember that the risk management process is iterative so that new risks need to be added as they arise and old risks retired. The key to risk control is to move early and decisively on problems and maintain flexibility in the approach to risks.

SPACECRAFT FAILURES

Once we have an understanding of what risks are and how they can be managed we can apply this intelligent approach to Smallsats. But where do we begin?

"It was almost a 100% success"

Quote from a spokesman from the Italian Space Agency after their tethered satellite experiment turned 25 kilometres of wire into a mass dummy in the belly of the shuttle.⁸

So where do the failures come from? How can there be any failures at all when traditional spacecraft spend inordinate amounts of money on S class parts that are screened, burned in, environmentally tested and then de-rated for all applications? It comes as no surprise to anyone in the Smallsat business that parts are not the

number one failure mechanism. Empirical evidence suggests there is an 80/20% split between Poor Design and Human Error.⁹

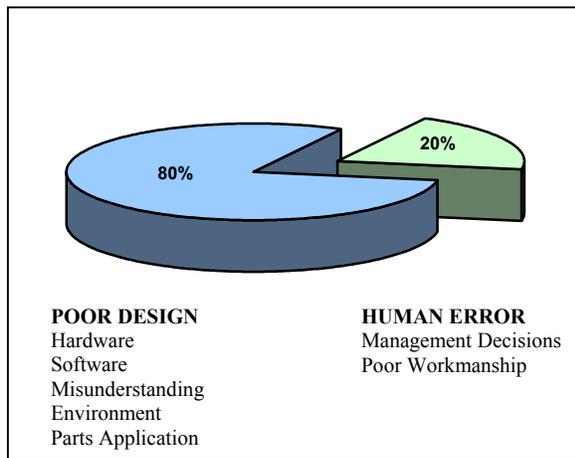


Figure 3. Spacecraft Failures

Poor Design – Hardware and Software

In 1979 the LEWIS satellite had an inadequate Guidance Navigation and Control System (GN&C) which caused the satellite to tumble out of control.

In 1999 the Mars Polar Lander was badly designed so that it could not withstand the shock of landing and the motors shut down.

Also in 1999 the WIRE satellite was lost as a starting transient caused the telescope covers to prematurely eject.¹⁰

The list goes on and on and the design failures are not limited to hardware design. With the increasing use of complex software there have been many instances of improperly tested software either locking up or in the case of the Clementine satellite switching on the thrusters and not being able to switch them off!

Poor Design - Misunderstanding the environment

Second on the list is not understanding the environment that the spacecraft has to endure on its journey through manufacture, to space and for its allotted life. I particularly mention the satellites life on the ground because this is an often-neglected area of risk. Satellites spend years in pieces, often scattered around the world before they are finally integrated in a relatively clean facility. During that long period they are exposed to all sorts of storage and transportation environments, heat, humidity and the exposure to humans who no matter how skilled often make mistakes.

The human environment is a danger. Less is heard about these failures because they are recoverable on the ground but the costs are still added to the final project total. The intelligent application of Quality Management and process can often eliminate these ground-based risks.

Once the spacecraft is complete it has to endure the severe vibration environment of launch and then the thermal cycling of on orbit operations. There have been numerous causes of launch failures associated with badly misjudged vibration environments in the launcher and separation systems.¹¹

Poor design – Parts Application

We now come to the one area that has the most money thrown at it over the ages and that is parts. Parts and in particular mechanical parts are the least likely items to fail in any space application. When people point to a part failure a little more analysis normally reveals that the part was exposed to a condition for which it was not designed such as an inrush current, over temperature or radiation dosage that exceeded its limits. In other words, there was a design problem or environment problem and not a problem with the part itself.



Figure 4. An expensive example of Human Error

Human Error –Management Decisions

The human error slice of the failure pie can be divided into two portions Management and workmanship. People decided to launch the shuttle when they knew the O rings were not designed to operate at low temperatures, people stood by as numerous instances of insulating foam broke off the external tanks of the Challenger, well before the actual disaster. These high profile examples illustrate deliberate decisions that ended in disaster.

Human Error – Workmanship

Finally, we come to the workmanship errors such as bad soldering, poor assembly techniques, bad processes that contribute to short or long term problems.

Having established the priorities of the failure mechanisms we can now explore more about the reliability and how to apply the correct amount of Quality Management effort to reduce the risks.

In the risk discussion we mentioned the need to avoid risky design and build slowly upon existing, proven technologies. We will now look at the arguments for using flight heritage as much as possible.

HERITAGE

One of the cornerstones of a Smallsat approach is to rely on flight and design heritage to avoid the cost and time involved in qualification testing. This approach is sound but must be used with caution.

Before heritage can be claimed it must be demonstrated that the design has sufficient margin on all the relevant technical parameters and over the duration of the mission. It is rare that two missions environmental conditions are identical as a simple change in the orbit characteristics can affect the radiation and thermal environment significantly.

A more stable and workable solution, and one adopted by most Small sat providers, is to have an evolutionary approach so that each follow-on satellite builds on the experiences of the last. Only small incremental changes are made with each new launch and the differences are identified at the requirements development stage for each new project.

This approach has many advantages. Radical and hence risky departures from a baseline are avoided, small changes are more manageable from a technical standpoint and by identifying the small changes early in the project life cycle they can be identified, tracked and mitigated in a risk budget.

If heritage designs do not fulfil the expectations there is a need to prove the new developments are capable of meeting the requirements and the designs must be qualified.

QUALIFICATION

Smallsat providers are faced with a dilemma when it comes to qualification. Qualification programs are hugely expensive, time consuming and require specialist knowledge and facilities. On the positive side

they give the customer and insurance underwriters the confidence they require to fund and insure the satellite mission. So how can we apply the required intelligence to reduce the risk and assure the quality and reliability of the spacecraft?

The on orbit environment of space is reasonably benign, getting there is not. The qualification route proves the spacecraft will survive all of the following:

- Vibration levels of launch (including acoustic vibration),
- Shock levels of separation,
- Quasi static loading,
- Thermal cycling experienced during orbit
- Radiation effects on electronics
- Outgassing effects from materials,
- Electromagnetic Compatibility (EMC)

And possibly mechanical problems like cold welding and lubrication issues associated with deployable structures.

Not only does the Smallsat have to work in a vacuum environment, it also has to work in worst-case conditions, if something goes wrong, and also for the entire mission duration.

Qualification not only proves the design will work it gives an assurance of the lifetime and long-term reliability.

A typical approach to qualification for Smallsats would follow the steps:

Avoid qualification if at all possible. This is not meant to be a glib statement but if there is a route to a qualified product without qualification testing it should be vigorously pursued. Rely on flight and design heritage wherever possible, exploit previous experience. Keep the design simple by avoiding any deployable structures. Use previously qualified processes and procedures, avoid the new and unknown and keep new development to a minimum.

If you have to qualify because previous heritage cannot match the exact environment then pursue a delta qualification campaign that will ‘make up the difference’.

For new development or for any other reason a full qualification campaign is required consider the following:

Test as early as possible with qualification or proto-flight models. This will mitigate the risk of failure and

allow alternative routes for supply or subcontract to be taken.

Ensure the qualification campaign addresses both short-term survival and long-term reliability. There are many standard accelerated life-testing techniques for both electrical and mechanical parts that can compress the expected life of years into months of testing.¹²

Always have a contingency plan in the event the testing fails. If there is a sign of failure on the horizon: act decisively and act quickly. Good project managers know things do not get better on their own and you will get the full support of Quality Management!

When things do go wrong during testing campaigns, follow the Material Review Board (MRB) process, it is always shorter and less expensive in the long run and the outcome will meet the requirements. Let Quality Management do its job!

Many Smallsat companies try to integrate to a high level before qualification testing. This can mean units and sub systems can be all integrated into the spacecraft before seeing the environmental testing conditions. This approach is attractive because of expediency but introduces risk and it is risk late in the integration program. This should only be tried if there is a high level of confidence in a design, there are alternatives and there is little new development.

As we have seen there have been major failures associated with poor software design we will now examine the Quality Management effort given to Software.

SOFTWARE QA (SQA)

Together with the use of commercial parts in Smallsats there is an equal desire to use Commercial Off The Shelf (COTS) software. Similar financial and schedule enticements are there for the eager project manager. Most COTS software does not stand up to any of the usual rigor expected for flight software but once again it is important to match the quality of the software to the application.

During the requirements stage the criticality of the software function must be assessed, similar criteria to hardware may be used where any software function that could cause damage to the spacecraft must be under maximum scrutiny.

The application of special techniques such as the ones established by the Software Engineering Institute and other industry "best practices" standards are used to

evaluate, monitor and assess the software development life cycle.

Critical Software

For critical software the complete software development lifecycle must be under control from the evaluation of the requirements through to the control of changes, the focus of effort should follow the guidelines of a recognized standard such as MIL STD 498 and the principal areas of control should be to:

- Identify Standards and Guidelines
- Evaluate Software Tools and facilities
- Evaluate Requirements Analysis Process
- Evaluate Design Process
- Evaluate Code and Unit Testing Process
- Evaluate Integration Testing Process
- Evaluate Acceptance Testing Process
- Evaluate the Corrective Action Process
- Evaluate Deviations and Waivers Process
- Evaluate Configuration Management Process

This will ensure that the customer's requirements are in agreement with the statement of work of each software contract.

Non-Critical software

Non-critical functions can use COTS or modified COTS software and the trend is to use up-loadable software and actually test and integrate the software on orbit. This has schedule advantages and offers a great deal of flexibility to upload and modify and improve the software on orbit but caution is required. It must be impossible to modify any boot software resident on the spacecraft (in non volatile memory) and once again it must be impossible to damage the spacecraft itself.

For any Smallsat program with a significant software component a Software Management Plan/Software Development Plan (SMP/SDP) is required to document a planned and systematic set of activities to ensure software processes and products conform to requirements, standards, and procedures.

PARTS SELECTION

Since the Gemini era when all and any electronic parts were scarce there was a concerted effort to improve the quality of spacecraft by developing highly reliable parts. Space (S) rated parts programs were refined by the aerospace industry, principally by NASA and the military, where traceability, testing and screening programs could assure the finished component would meet the most exacting demands of the space

environment. S rated parts are highly reliable and their production and testing history can be tracked all the way to the copper mines of Peru but they are also orders of magnitude more expensive and difficult to get hold of because of the long lead times. S rated parts come in low volume, have limited functionality, are highly reliable (and have proven reliability) but are very expensive.

The seventies and eighties saw commercial forces that increased the market demand for cheap, high volume consumer electronics and now in the new millennium cell phones, PCs and personal entertainment systems are available at increasingly less cost. So we have commercial parts with exceedingly high volume, high functionality, high reliability in a benign environment, and they are readily available and exceedingly cheap.

Now no one is suggesting we gut the Sony Walkman and launch the contents but it is easy to see the enticing argument for the use of commercial parts. To temper the program manager's enthusiasm who has a limited budget and time pressures to complete a product a healthy dose of reality needs to be applied and this is where Quality Management can add value.

As we have seen parts are important, not as important as correct design, the environment or assembly, but they are still important and it would be totally foolhardy to follow the mantra of commercial parts without looking at the application, the mission duration and the environment.

Critical functions still require the best available parts and redundancy of application should not be used just to allow for the unreliability of a series of parts. The satellite downlink transmitter has to work, it has to work every time. It has to survive the vibration of launch, the thermal cycling of every orbit, the radiation environment, the constant switching on and off and it has to do it for, typically, 5 years or more.

Assessing the criticality of the various functions of the spacecraft at the design stage is crucial. An example of Severity Categories is given in Table 2.

Table 2. Severity Categories

Category	Severity Definition
1	Catastrophic failure modes that could result in loss of the spacecraft.
1R	Failure modes of redundant hardware items that, if failed, could result in category 1 effects.
1S	Failure in safety or hazard monitoring systems that could lead to Severity Category 1 consequences.
2	Critical Failure modes that could result in loss of one or more mission objectives.
2R	Failure modes of redundant hardware items that could result in Category 2 effects.
3	Marginal failure modes that could cause degradation to mission objectives
4	Negligible failure modes that could result in insignificant or no loss to mission objectives.

Failure Mode Effect Analysis (FMEA) procedures should be performed in accordance with documented procedures. Failure modes resulting in Severity Categories 1, 1R, 1S, or 2 should be analyzed in greater depth, to the single parts if necessary, to identify the cause of the failure.

Results of the FMEA will be used to evaluate the design relative to the requirements (for example, no single unit failure to prevent removal of power from the unit). Identified discrepancies will be evaluated by the management, Quality and design groups to assess the need for corrective action.

The FMEA will analyze redundancies to ensure that redundant paths are isolated or protected such that any single failure that causes the loss of a functional path will not affect the other functional path(s) or the capability to switch operation to that redundant path.

All failure modes that are assigned Severity Categories 1, 1R, 1S, and 2 will be itemized on a Critical Items List (CIL) and submitted with the FMEA report. Rational for retaining the items will be included on the CIL.

These analysis techniques are a useful way of applying the right amount of design effort and enable the astute program manager to assess and react to the risk.

The analysis will reveal the criticality of the application within the spacecraft and hence the suitability of a COTS part can be assessed. The environmental considerations include:

- Radiation susceptibility (TID, SEU)
- Temperature constraints
- Shock
- Vibration

For reliability the use of parts from NASA or ESA standard parts lists is the best option.

There are a number of more subtle failure modes that can have a long-term effect on spacecraft reliability.

What are the packaging failure modes for COTS? Humidity based corrosion and inter metallic failures are well understood and documented. The failures are time dependent and latent in nature, and testing may not reveal either corrosion or purple plaque, until it is too late.

If the part is to be used in an optical mission have outgassing properties been assessed?

It is a fact that the use of COTS parts in “optical” sensitive areas is troublesome, many contain indeterminate materials and it is necessary to determine the outgassing properties of the part by test, and find appropriate engineering solutions.

COMMERCIAL RELIABILITY AND COST

Although it is extremely enticing, to choose COTS parts because of their immediate cost savings, to understand the true reliability of COTS parts we have to consider the following:

The infant mortality region has to be eliminated. COTS parts are not screened they do not undergo pre-cap inspections, PIND, X-rays, C SCAN, burn-in, or environmental testing for the few percent of early failures.

Pi Q factors (quality multiplier coefficients for failure rates) can be hundred of times higher for unscreened commercial parts compared to screened parts.

Steady State (constant) failure rates are higher compared to military high-reliability parts. This is due

to packaging technologies, metallization technologies, design rules and margin of safety for electro migration. Has the life expectancy under de-rated conditions been assessed?

Has the Thermal cycle durability of lead free solder joints, especially surface mount technology been examined?

On the programmatic side. How are design changes managed, is there process control and what screening, if any, is applied?

How is obsolescence managed, how reliable is the supply chain?

JPL has stated “Acquisition costs of COTS in high reliability applications do not reflect total cost of ownership”.¹³

JPL also quotes numbers of total cost of ownership to be between 40 – 50 times the costs of the COTS acquisition, and finally JPL quotes COTS yield as 58%

COTS devices are also constantly reengineered, with a typical cycle times of 18 months. The main scope of this fine-tuning is to optimise the design (remove spare margin, tweak the timing circuitry, additional functionality). All this is going on without the buyer being informed of any of the changes that are taking place. The problem with this is that the original part may not be available for new hardware, and on top of this, the new chip (although supposedly better) may not work in the old design. Needless to say that re-qualification will be required (including radiation testing), costing time and money.

One obvious solution is to buy sufficient spare parts at the outset of any new program, the drawback being the extra cost of buying, storing, and retesting.

Be very cautious in the application of COTS parts, the up front costs rarely reflect the true cost to the program.

As well as the intelligent use of parts, the use of process is often under scrutiny. One process that should not be compromised in a Smallsat program is the Material Review Board and the independence of Quality Management.

THE INDEPENDENCE OF QUALITY DECISIONS

Effective organisations always maintain an independent assessment of quality. ISO 9000

requires that quality decisions can only be useful if they are independent from cost and schedule pressures.¹⁴

While there were many technical failures with the shuttle Columbia in 2003 one of the strongest conclusions from the Columbia accident investigation report was that an erosion of the quality organisation made real quality decisions impossible.¹⁵

At NASA the Quality organisation was dependant upon the individual project for funding and the political pressure to make decisions based on political and schedule pressures was overwhelming. The 'Can Do' culture prevailed and the Quality role was reduced to a mere signature on the documents. Quality Management even reported to the project in many cases so the impetus to 'do the right thing' was minimized.

The report also concluded that the changes in corporate culture necessary to regain a truly independent status for Quality Management would be one of the hardest cultural shifts NASA had to undertake. The results of the 1986 Challenger disaster investigation uncovered the same organisational flaws and the problems were repeated 7 years later.¹⁶

Now, of course, the failure of a Smallsat does not have the same grave and tragic consequences as a Shuttle disaster but no one wants a mission to fail. If safeguards can be put in place to ensure that the quality of the end product meets or exceeds the requirements for a successful mission, and the cost is reasonable, it should be done.

Quality independence is easy to specify and quite easy to implement in the early phases of the program when cost and schedule pressures are less noticeable. The real test comes when there is a failure during flight acceptance testing and there could be a real impact on the program.

Traditional methods employ a system of Material Review Boards (MRBs) chaired by Quality Management who make decisions based solely on quality criteria. The Chair collects the technical inputs and charts a course of failure investigation or corrective action that will put the hardware back into a flight worthy state. He does this without the influence of the project managers who are concerned with cost and schedule. Quality is the number one concern. The MRB can only be effective if the chair has the authority and independence to make the right decisions (A certain dogged determination and insensitivity is also an asset!).

To ensure the success of the MRB there are two overriding requirements, the independence, as we have seen, and this means the MRB chair reports to a Quality manager/ director outside of the project and secondly the project itself must believe in the process and accept the decisions with little or no dispute.

There is rarely a case when 'doing it right' has not saved time and money in the long run.

Smallsats are no different and if there is one area of quality that should not be compromised it is with the MRB process. Keep the independence, keep the process and allow the chairman to make the quality decisions that will, eventually, get the satellite program back on track.

FROM ANALYSIS TO EMPIRICISM

Traditional space programs have relied heavily on analysis of any design. There have been many reasons for this. Many of the satellites have broken new technological ground and the customers have demanded an assurance that the new technology would function. The risk-averse culture of the space business that was started with the manned space program has often spilled over into the non-manned area. Most missions are complex and all have relatively high budgets, the time scales are long and the cost of failure high both in reputation and in dollars. So, naturally, assurance is required. Next we have insurance, the possibility of offsetting a potential loss by underwriting some or all of the cost of a failure during launch and operations. Second to engineers, the underwriters are probably the most cautious group when it comes to risk. To get their assurance they have demanded serious and credible proof that the satellite will perform.

Add onto this the environmental testing that all spacecraft are subjected to and you have a body of knowledge that helps enormously to allay the fears. So far, so good but what are the disadvantages of analysis.

Firstly it is expensive. To properly perform a Failure analysis, Derating analysis, structural analysis, Worst case analysis on all the myriad components in a satellite takes a huge amount of time and effort. It requires specialist skills, sophisticated software tools and a considerable amount of time.

Secondly, the outputs are often in doubt. Now I am not for one moment suggesting the analysis is not worthwhile but its results often have to be tempered with a heavy dose of common sense. A FMEA, for example, based on MIL HDBK 217 often arrives at overly conservative results. The handbook served its

purpose nobly when technology was not accelerating at its current exponential rate but now the reliability figures just cannot keep up with the technology and many commercial devices are just not included.

The reliability of the shuttle was analysed, using all the best methods available, as being capable of 20,000 flights without a fatal accident, it lasted 26.

There are numerous commercial standards available (Bellcore ETC), which have the reliability data and methods, but how will our nervous underwriters and penny-wise customers be assured that the product is not going to fail?

The suggestion is that analysis can be used in conjunction with heritage data and a rigorous testing campaign, in other words the analysis complements the overall package of data that is required to give the confidence in the design.

But what is the reliability of my spacecraft? I hear the customer cry in amazement. I don't have a reliability figure, who can assure me it will last for five years? And this is where the true paradigm shift of Smallsat thinking comes into play. You may never be able to give a firm number. The confidence is built up though the reliance on a robust design based on functions with known heritage, a few carefully scrutinised changes, a sound knowledge of the environment in which the Spacecraft will operate, a parts program that matches the quality to the function and more importantly a testing campaign that will screen out risks at a very early stage. The traditional analysis has moved from its pedestal of supremacy to a supporting role, which now verifies the results of testing

CONCLUSIONS

This paper has argued that the intelligent application of Quality Management principles to a Smallsat project can greatly enhance the chances of a successful mission. The key is to manage risk appropriately, to carefully identify the risks, analyse them and then adopt active strategies for their mitigation. By applying the appropriate amount of process and diligence at the requirements and design stages, areas that require the most scrutiny, the project manager can avoid or eliminate mission reliability or performance issues. With the selection of appropriate parts and testing strategies high levels of confidence can be gained in the reliability of the spacecraft and the insurers will feel confident in the mission outcomes.

Quality Management can be a forceful tool to realise everyone's dream of easier, affordable access to space, the key is to apply the principles with intelligence.

Acronyms

CDR	Critical Design Review
CIL	Critical Items List
COTS	Commercial Off The Shelf
C SCAN	Ultrasonic, non-invasive inspection
DPA	Destructive Physical Analysis
EMC	Electromagnetic Compatibility
EOL	End Of Life
ESA	European Space Agency
FBC	Faster Better Cheaper
FMEA	Failure Mode Effect Analysis
FMECA	Failure Mode and Effect Criticality Analysis
IC	Integrated Circuit
ISO	International Standards Organization
PA	Product Assurance
PC	Personal Computer
PCB	Printed Circuit Board
PDR	Preliminary Design Review
QA	Quality Assurance
QML/QPL	Qualified Materials/Parts List
QM	Quality Management
RE	Risk Exposure
RFP	Request for Proposal
MRB	Material Review Board
NASA	National Aeronautics and Space Administration
PEMs	Plastic Encapsulated Modules
PIND	Particle Impact Noise Detection
PiQ	Quality factor for parts
RE	Risk Exposure
SDP/SMP	Software Development Plan/Software Management Plan
SEU	Single Event Upset
SOW	Statement of Work
SQA	Software Quality Assurance
SQM	Structural Qualification Model
TID	Total Ionizing Dose
TPM	Technical Performance Measurements
T & Cs	Terms and Conditions
WBS	Work Breakdown Structure
WCA	Worst Case Analysis

References:

1. <http://history.nasa.gov/moondec.html>
2. <http://techdigest.jhuapl.edu/td2201/goldin.pdf>
3. <http://www.spaceref.com/news/viewnews.html?id=864>
4. <http://www.spaceref.com/news/viewnews.html?id=680>
5. Reference System Engineering Management Benjamin S Blanchard 2nd Edition John Wiley and Sons 1998)
6. Boehm's "top 10" risk list, (Boehm, B. IEEE Tutorial on Software Risk Management. IEEE Computer Society Press, 1989.).
7. "Risk Radar" tool
www.iceincusa.com/products_tools.htm
8. <http://www.globalsecurity.org/space/world/italy/tss.htm#ref50>)
9. Logic of Microspace, Rick Fleeter, Microcosm Press/Kluwer Academic Publishers 2000
10. <file:///C:/Documents%20and%20Settings/bcox/Local%20Settings/Temporary%20Internet%20Files/Content.IE5/3RKCTCQA/256,1,Slide 1>
11. http://www.aviationnow.com/media/pdf/spec05_launchfailures.pdf
12. http://www.weibull.com/AccelTestWeb/arrhenius_relationship_introduction.htm
13. http://parts.jpl.nasa.gov/cots/external/issues_1.pdf
14. <http://www.iso.org/iso/en/iso9000-14000/iso9000/iso9000index.html>
15. http://www.nasa.gov/columbia/caib/html/images/images/caib_07.jpg
16. <http://www.engineering.com/content/ContentDisplay?contentId=41009024>

Additional Reference Material

Space Missions Analysis and Design, James Wertz & Wiley Larson, 3rd Edition Microcosm Press/Kluwer Academic Publishers 1999.

Understanding Space, Jerry Jon Sellers, 2nd Edition McGraw Hill 2000

Elements of Spacecraft Design, Charles D Brown, AIAA Education series, 2002

<file:///C:/Documents%20and%20Settings/bcox/Local%20Settings/Temporary%20Internet%20Files/Content.IE5/JX7891O3/256,3,Program Risk Management>

Waltzing with Bears: Managing Risk on Software Projects, Tom DeMarco, Timothy Lister. Dorset House 2003.

The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA - Diane Vaughan, University of Chicago Press, 1997

Texts by McConnell, Gilb, Humphrey, Pfleeger, Blanchard all have sections on risk management