Available online at www.sciencedirect.com
SCIENCE DIRECT®
PERGAMON
Acta Astronautica 54 (2003) 221–228
ACTA ASTRONAUTICA
www.elsevier.com/locate/actaastro

Risk management for micro-satellite design☆

Fabio Santoni*

Scuola di Ingegneria Aerospaziale, Università degli Studi di Roma "la Sapienza", Via Eudossiana 16 00184 Rome, Italy

Received 12 December 1999; accepted 27 October 2002

Abstract

It is shown how the methods of risk analysis have been used in the University of Rome micro-satellite program. One of the driving research topics related to this program is the reduction of cost in building spacecraft. The probability risk analysis techniques seem to be a powerful tool in the field of micro-satellites design, to outline possible faults. Innovation and limited budget forcing the designer to move in a very "risky" environment and can be faced with an as rigorous as possible decision making method.

In our project, cost reduction is often attained relying on commercial, not space-rated components, which of course increases risk. This is why the design process should be led by the careful analysis of the risk associated with the selection of components and construction techniques.

In standard applications risk can be evaluated from reliability data obtained in previous and well known similar applications. In our case, for many components, there is a lack of reliability data, due to the obvious missing experience when dealing with not yet space qualified, or even never flown before components. This lack is overcome using numerical simulations and practical engineering considerations, but does not allow a rigorous reliability assessment.

A simple qualitative analysis is used to rank priorities among subsystems and allocate economic resources and development efforts. The main risk source is space radiation effect on CMOS electronic components. Therefore, development resources are directed to radiation effect mitigation. A procedure is proposed to lower risk without using space rated components.

1. Introduction

Micro-satellites have become more and more attractive in last years. They offer an advantageous support for testing "state of the art" technology with short time to launch and reduced cost. Moreover, this class of satellites is particularly suited for educational purposes. Many Universities have successfully launched and operate micro-satellites. Also, Università di Roma "la Sapienza" is currently designing its own micro-satellite, in the frame of a national program which involves several Italian Universities.

The Università di Roma micro-satellite program [1] was established with the aim to build a very simple, "general purpose" satellite bus, to give scientists a low-cost possibility to conduct small scientific in orbit experiments, and also to give our students a more effective technical education through hands-on experience. Many of the design principles and driving aspects are based on SAPPHIRE and OPAL satellites, developed at Stanford University Space System Development Laboratory [2,3].

☆ Paper 1AA-97-1AA.6.2.03 presented at the 48th International Astronautical Congress, October 6–10, 1997, Turin, Italy.

* Tel.: +39-644585334; fax: +39-644585952.
E-mail address: fabio.santoni@uniroma1.it (F. Santoni).

0094-5765/03/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/S0094-5765(02)00291-6

In University micro-satellite programs, like ours, risk is mainly due to two factors: limited funding and the use of "new", and often not yet space qualified, state of the art technology. Limited funding granted to Universities for educational programs often do not allow to use first quality components for every subsystem. In many cases one is forced to fly components designed and built for terrestrial application because they are much cheaper. These components must be modified and adapted to fulfill the requirements imposed by the launch and the space environments. Testing new technology adds, of course, risk associated with unforeseen and eventually unknown behaviours.

Risk assessment in the micro-satellite field is a quite ambiguous task, due to the lack of a consolidated experience and to the fact that micro-satellite technology is evolving very fast. But it does not mean that it is impossible or of no advantage to use the methods of probabilistic risk analysis in micro-satellite design. When it is necessary to rely upon new technologies or on cheap components, it is very important to identify which areas of the system can be safely built by off the shelf terrestrial technology to allocate more budget or development efforts where space rated components are indispensable. To meet the goals of the project and to take conscious decisions one needs to set up a rigorous process for components and construction techniques selection by evaluating in some way the associated risk. Interest is not to attain a prefixed reliability or to assess it, but in getting the maximum reliability allowed by cost, weight and development time constraints.

Starting from a basic design satisfying minimum requirements, by simulations or collection of available data, design is refined improving the most critical parts.

2. Description of the system

A brief description of the starting design configuration is given, in order to clarify the assumptions made in the risk analysis model.

Scheduled mission lifetime is one year. This is, of course, only a reference duration, depending on the payload requirements. Many payloads have been proposed and studied, but a definitive choice has not been done. As said, the main interest is in the satellite "bus" that should be easily adjusted to support different kind of payloads.

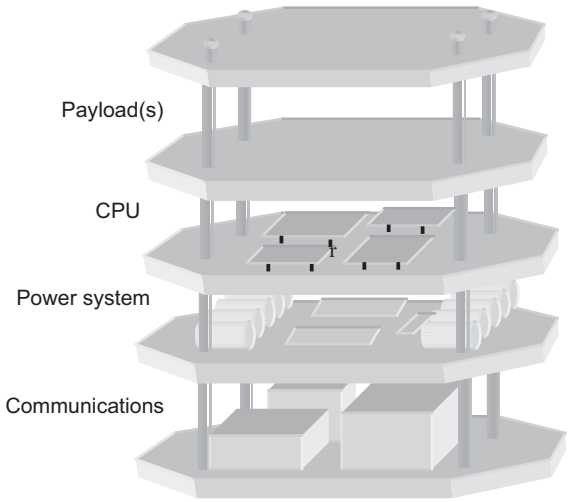

Fig. 1. Satellite structure and components.

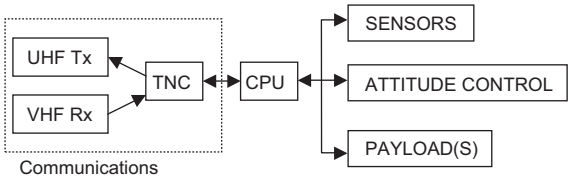

Fig. 2. System block diagram.

The satellite is an octagonal prism, 16 cm side, 25 cm height. The structure is primarily made of aluminum sandwich panels, disposed in "trays", on which the boxes containing all the equipment internal to the satellite are fixed. Four stainless steel rods keep all the trays together, as illustrated in Fig. 1. Also the sides of the prism are made of aluminium sandwich panels. They give the structure the necessary torsion stiffness and offer a support for the solar panels. Launcher separation mechanism has been designed for compatibility with many launchers. Separation is obtained using a *frangibolt* activated by a thermal battery, instead of classical pyrotechnic devices [4].

The block diagram of the on-board electronics is illustrated in Fig. 2.

The communication subsystem consists of one VHF receiver, one UHF transmitter, and a terminal node

Table 1
Budget allocation among subsystems ($)

Subsystem	Launch	Hardware	Total	
Communications	2900	800	3700	2.9%
CPU	1100	800	1900	1.5%
Power	10,100	70,200	80,300	64.0%
ACS	6400	2600	9000	7.2%
Structure	24,000	1200	25,200	20.1%
Harness	2200	500	2700	2.2%
Sensors	200	2500	2800	2.2%
Total satellite estimated cost	46,900	78,650	125,600	

controller (TNC). This last unit is used for digital data communication. It organises data in packets according to Amateur Packet AX.25 protocol and provides the modulation/demodulation function for interfacing with transmitter and receiver. TNC settings and communication protocol are stored in a ROM memory. A RAM memory is also available to the TNC for temporary data storage. All the components are "off the shelf" and have proved to be reliably used in terrestrial applications.

The on board computer system (CPU) is also assembled with not space rated components. The microprocessor, a Motorola 68332, RAM and ROM memory chips and all the peripherals (Analog to Digital and Digital to Analog Converters, sensor data multiplexers) are commonly used in terrestrial robotics applications. Numerical simulations and literature data show that use of an error detection and correction (EDAC) system is indispensable to prevent commercial RAM memories data corruption by space radiation effects. In heliosynchronous orbit, the single event effects (SEE) frequency is as high as two SEE per orbit when crossing in the South Atlantic region [5]. Such a frequency does not allow reliable mission operations. It could be necessary to reset the CPU too often, and there is also high risk of wrong actions execution by the system. The satellite EDAC hardware is currently being developed.

Power system consists of solar panels, one battery made of 10 4Ah NiCd cells, with 12 V nominal voltage. A 5 V bus is obtained from the 12 V through a dc–dc regulator.

The satellite is spin stabilised. Attitude manoeuvres are possible using two magnetic actuators made of vacuum core coils. Attitude determination is achieved by a three axis magnetometer, earth sensors, and solar panels current, which give information on the sun direction.

Thermal control is passively achieved, by applying adhesive tapes on the external surfaces [6]. On board temperature is monitored by temperature sensors, which are the main part of telemetry data, together with solar panels currents.

Payload interface to the bus consists of digital control output lines from CPU, for payload command, data lines for collecting experiment results.

Table 1 illustrates resources allocation for the system, showing the contribution of every subsystem to launch and hardware cost, assuming a launch cost of 3000$/kg.

Cost is mainly due to solar panels and launch. Being a research and education program, University of Rome hopes to have access to reduced cost, or even free, launch opportunities and to receive industry donations for solar panels. If these opportunities will be offered, satellite cost lowers to a fraction of the initial cost (less than 9000$).

3. Risk analysis model

The analysis is carried on with the main purpose to rank priorities in the design process and to outline possible improvements in resources allocation for University of Rome micro-satellite, that allow to

maximise the reliability of the satellite bus, remaining within the constraints imposed by the limited budget. Payload is not included in the analysis, because the bus can support different payloads, that are currently being studied. Payload missions will, of course, benefit of eventual improvements in the bus.

The risk analysis model used is a *qualitative* failure mode and effect criticality analysis (FMECA) [7]. Even if the design is not at an early stage, following SSDL experience, and many components have already been selected, it is not possible to use a quantitative reliability model in assessing risk. All the components are commercial class and failure rates are rarely available. Any quantification of failure probability would have very poor confidence and the results would not give more insight than a simple qualitative analysis. To assess reliability with the necessary confidence level, it is necessary to collect many experimental data from numerous and costly tests, that make assessing mission reliability impractical. This is not a main concern in University of Rome micro-satellite. Tests have been done, for example, to validate the structure mathematical model. Thermal vacuum and vibration tests have been done at Stanford on a similar structure, but data are not enough for quantitative reliability assessment.

The simple qualitative analysis illustrated below, supported by the available data, tests and simulations, is thought to be appropriate for ranking priorities in resources allocation.

Three probability levels and three severity levels. for identified failures are considered. They are assigned on the basis of engineering considerations, previous experience in actually flown components, numerical simulations or experimental tests. A slightly different approach will be followed with respect to space radiation effects on electronics hardware, because the results of numerical simulations and literature data are directly expressed as single event effect (SEE) per day, which translates immediately in components failure rate.

The three failure probability levels are:

A. very high,
B. high,
C. low.

Failure severity levels are assigned according to the relevance on the whole mission failure:

Table 2
Criticality

		Probability		
		A	B	C
Severity	α	α A	α B	α C
	β	β A	β B	β C
	γ	γ A	γ B	γ C

α fatal (loss of mission),
β major,
γ minor.

The criticality matrix (Table 2) is the result of the combination of failures probability and severity.

Criticality scale is thus as follows:

C1. α A,
C2. α B $= \beta$ A,
C3. β B,
C4. α C $= \gamma$ A,
C5. β C $= \gamma$ B,
C6. γ C.

Failure modes ranking is done according to their criticality. In this way a fatal failure, which has low probability to happen, is ranked less critical than a medium severity failure which is very likely to happen.

Interrelations between failure modes are not considered, because it is assumed that there always is only one FM that happens first, and that may eventually cause other failures to arise. This means, for example, that thermal control failure or communications link failures due to malfunctioning of the attitude control system, will be considered as attitude control failure only.

The satellite system components can be conceptually organised in subsystems. The reliability diagram is the series of all the subsystems.

First a ranking among the subsystem according to their criticality is done. Then for each subsystem a qualitative FMECA addresses the most critical components which contribute to the subsystem failure.

4. Quantification of the risk

The method shown before is used to assess the contribution of every subsystem to the overall risk.

The analysis starts from the base design configuration discussed in the system description.

Use of commercial plastic electronics chips is not considered to affect the system reliability. Plastic integrated circuits have shown to be reliably used also in aerospace and military applications, because many manufacturers ensure reliability levels for commercial components that are comparable with military standards components [8].

Ground Station failure is not included in the analysis, because it is a repairable equipment and redundancy is also easily attainable by existing radio amateurs satellite stations.

Table 3 shows the probability, severity and criticality assessment for the satellite subsystems.

Even with an EDAC system to prevent from SEE in the CPU RAM, the radiation environment still seems to be the main problem for on-board electronics. According to simulations [9], both the CPU and TNC ROM memories, in which the code is stored, have a very high SEE frequency. Using tantalum or lead spot shielding, the frequency is 0.0209 SEE/day for the CPU and 0.0095 SEE/day for TNC in heliosynchronous orbit.

This is an average frequency. SEE are generated by the high-energy particles in the Van Allen belts. Even if SEE mainly happen in the polar and South Atlantic regions, it is possible to assume a constant rate over the orbit. Moreover, there is no correlation among subsequent SEE. A Poisson distribution can be used to give an estimate of the time between SEE, which is assumed here as a worst case mean time between failure (MTBF) for ROM devices, which corresponds to the average probabilistic satellite lifetime. The MTBF obtained for the CPU and TNC memories can be evaluated from the SEE frequency. The results are in Table 4, for heliosynchronous orbit and a MIR station orbit.

This is a conservative estimation, because, at least for CPU, the code is copied from ROM to EDAC protected RAM at launcher separation switch on. Thus, as long as CPU is not remotely reset, possible ROM SEE have no effect. If a remote reset occurs, the code starts again from ROM and this is the situation in which ROM SEE can actually be dangerous. Taking this into account, the MTBF is the combination of a SEE and of a remote reset possibility. Reset of the CPU should be quite a rare event, according to the laboratory experience with the software developed till now. Anyway it is not possible to estimate the reset probability in orbit, so the worst case must be considered. This is why Communications and CPU subsystems are given the highest probability of failure.

Table 3
Subsystems criticality

Subsystem	Probability	Severity	Criticality
Communications	A	α	C1
CPU	A	α	C1
Harness	B	α	C2
Power	B	α	C2
Thermal	B	β	C3
Payload interface	C	α	C4
Launcher interface	C	α	C4
Structure	C	α	C4
ACS	C	α-(β)	C4-(C5)
Sensors	C	γ	C6

Table 4
Estimate of ROMs MTBF (days)

	Helio-synchronous orbit	Mir station orbit
CPU ROM	48	219.23
TNC ROM	105	483

Harness failure is medium probability. Possible faults are wires unsoldering and connectors failure. Probability is high because of the number of wires and connectors used in the satellite. Not all the connections have the same severity. As a worst-case approximation, all the wires are given a class α severity.

Power failure is medium probability because batteries have been dimensioned for a lifetime slightly longer than 1 year in ideal thermal environment and discharge conditions. This saves power subsystem weight, but increase risk in case of loss of slight deviation from nominal conditions.

Thermal is medium failure probability because the uncertainties in the thermal design might cause the temperatures to deviate slightly from nominal. This is considered a degradation of the mission, because working could be intermittent, batteries lifetime and solar panels efficiency might be reduced. Probability of reaching temperatures fatal for the electronic equipment is low.

Table 5
CPU failure modes criticality

Failure mode	Probability	Severity	Criticality
Permanent SEE in CPU ROM memories	A	α	C1
Fatal software "bug"	C	α	C4
Permanent SEE in micro-processor	C	α	C4
SEE in microprocessor and remote reset failure	C	α	C4
Double bit error in CPU RAM memories, not recoverable by EDAC	C	α	C4

Table 6
Communications failure modes criticality

Failure mode	Probability	Severity	Criticality
Permanent SEE in TNC ROM	A	α	C1
Transmitter final amplifier transistor failure	B	α	C2
Short in transmission lines or antennas	C	α	C4
Receiver failure	C	α	C4
Permanent SEE in TNC micro-processor	C	α	C4
Antennas deformation, or not correct deploying	C	β	C5

Attitude control system is low failure probability because hardware is quite simple. Coils are passive components and no integrated components are used in the coils switching system. Attitude sensing is distributed among magnetometer, earth sensor, and sun sensing through solar panels current. Severity depends mostly on payload requirements. It is *fatal* if payload requires attitude stabilisation, otherwise it is *major*, because of the consequences on the thermal system, which is designed exploiting spin effect on heat inputs distribution.

Payload interface consists of digital control output lines from the CPU, for payload command, and data lines for collecting experiment results. Probability of failure is low. Criticality is α, because failures might be fatal to the mission objective.

Launcher interface failure probability is mainly due to *frangibolt* or thermal battery failure. Probability is low, but severity is high, because failure is fatal to the mission. Also structure is not likely to fail. It is a very compact design and there are no mechanisms or extendible parts. Severity is high.

Sensors are low failure probability and also low severity, because loss of few temperatures or panel current lines does not affect payload.

4.1. Subsystems components criticality

An analysis similar to the one conducted for the entire system is applied to a subsystems level, to identify the most critical components. This allows to reduce subsystem contribution to the overall risk in the most effective way.

Tables 5 and 6 show the analysis done for the most critical systems.

5. Design alternatives according to components criticality

The results of the criticality analysis show that the main concern is space radiation effects on commercial MOS technology electronic components. Radiation effects on CPU RAM can be mitigated by inexpensive EDAC microcircuit. There is no need for TNC RAM protection, because few data are stored and the most critical event is loss of some telemetry or payload data, which is not highly critical to the mission.

CPU and TNC ROM memories seem the most critical components and possibly resources should be allocated in this direction. Using radiation hardened ROMs is, of course, the most effective solution, but with very high cost. Different approaches could be either avoid using ROMs in which SEE might have occurred, or introducing redundancies in the system, still using low cost commercial components.

The first approach can be used for the CPU subsystem. It possible to execute the on-board code from ROM only once, at separation, when ROM has not been exposed to radiation environment for a long time and the code has a high probability to be safe. Then the on-board code is copied on the static RAM memories, protected by EDAC. The ROM is disabled at this point. On remote reset, code can be run from RAM, since information stored on static RAM is kept, as long as power is applied. This procedure looks almost risk

Table 7
Estimate of redundant TNC MTBF (days)

	MTBF	1 year mission failure probability (%)
Heliosynchronous orbit	157	90%
MIR station orbit	724	40%

Table 8
Estimate of MTBF for stand-by redundant G3RUH modem

	MTBF	1 year mission failure probability (%)
Heliosynchronous orbit	631	44
MIR station orbit	1507	22

safe, because RAM memory is continuously "washed" by the EDAC system. Implementation is simple and inexpensive.

The procedure adopted for the CPU, in which the ROM is bypassed after the first switch-on and EDAC protected RAM is used, cannot be applied to TNC, because a proprietary, not modifiable code is implemented. Moreover hardware and software modifications to install EDAC on the Kantronics TNC are impractical.

Low cost of TNC suggests using a stand-by redundant unit, that should be activated autonomously by the CPU, if faulty TNC behaviour is detected. Autonomous detection is necessary, because with a TNC failure is not possible to communicate with the satellite from ground. TNC redundancy lowers risk, with two main drawbacks. First, a reliable algorithm should be set up to detect TNC faults. Second, the stand-by TNC is exposed to radiation during the stand-by time, so that the stand-by TNC might not be free of SEE when switched on. The MTBF for such a stand by configuration is only 3/2 the MTBF with no redundancy [10]. Table 7 shows MTBF and failure probability in 1 year lifetime, which is too high for reliable operation. Thus TNC stand-by redundancy does not significantly improve the satellite lifetime.

An alternative solution can be found considering that TNC has the two main functions to encode data according to the AX.25 protocol and to modulate/demodulate data.

These two functions can be split, making the CPU implement the AX.25 protocol, and using a commercial off the shelf 9600 baud MODEM, like the G3RUH [11], for modulation and demodulation. In this way protocol execution is safe, but a ROM memory is still used in G3RUH design, as the main part of a digital filter. It is smaller size than the one employed in the *Kantronics KPC-9612*. This lessen the SEE frequency because of the increased bit surface. MTBF for stand-by redundant G3RUH MODEMs can be evaluated from data available for the Kantronics. Results are in Table 8. This solution is not acceptable for reliable flight operations.

Elimination of the G3RUH ROM can be achieved using a microprocessor like the one used in the CPU system, with ROM for start up and EDAC protected RAM for safe reset. Of course this microprocessor is used to a fraction of its possible performance, but it is cost effective from software and hardware development viewpoint, using the same hardware architecture used for the CPU.

Solved for the most critical items, improvements are still possible to reduce failure criticality.

Batteries failure probability can be reduced to safe level by using bigger capacity cells or by using a redundant battery system to allow charge and discharge conditioning. Both increase weight, but the second possibility adds switching and control circuitry, that might lower the system reliability.

Another possible improvement is in the communications subsystem, where the final transistor amplifier can be inexpensively dimensioned in excess of load conditions, which ensure a much longer lifetime.

Acknowledgements

The author wishes to express sincere appreciation to Prof. Robert J. Twiggs, director of Stanford University Space Systems Development Laboratory (SSDL), for his open minded leadership, which offered the author the opportunity to spend 1 year at SSDL, where the idea of this paper matured, and for the determinant impulse given to the University of Rome micro-satellite program. Sincere appreciation goes also to all the SSDL members and mentors for their friendship and for the helpful suggestions and interesting discussions.

References

[1] F. Graziani, P. Teofilatto, F. Santoni, G. Palmerini, M. Ferrante, S. Secca, The Micro-satellite Program at Università di Roma "La Sapienza", Paper IAA-97-IAA.11.1.03, 48th LAF Congress, Torino, Italy, October 1997.

[2] C.A. Kitts, R.J. Twiggs, The Satellite QUIck Research Testbed (SQUIRT) Program, Proceedings of the 8th Annual AIAA/USU Conference on Small Satellites, Logan, Utah, 1994.

[3] http://aa.stanford.edu/~ssdl/projects.

[4] Nordt, Design of the SAPPHIRE Separation System and Launch Vehicle Interface, Ninth Annual AIAA/USU Conference on Small Satellites, Logan, Utah, 1995.

[5] L. Adams, R. Harboe-Sorensen, E. Daly, J. Ward, Proton induced upsets in the low altitude polar orbit, IEEE Transactions on nuclear science, 36 (1989).

[6] F. Santoni, Il microsatellite universitario UNISAT: studio del sistema di controllo termico, XIV Congresso Nazionale AIDAA, Napoli, Italy, 1997, pp. 2339–2343.

[7] O'Connor, Practical Reliability Engineering, 2nd Edition, Wiley, New York, 1985, pp. 129–130.

[8] W.L. Shultz, S. Gottesfeld, Reliability considerations for using plastic encapsulate microcircuits in military applications, Harris Semiconductor. http://rel.semi.harris.com/docs/rel/PEM/Mil_plas_1.html

[9] G.B. Palmerini, F. Pizzirani, Design of the Radiation Shielding for a microsatellite, Paper IAF-97-I.3.07, 48th IAF Congress, Torino, Italy, October 1997.

[10] S. Chiesa, Affidabilità, sicurezza e manutenzione nel progetto dei sistemi, C.L.U.T., Torino, Italy, 1990, pp. 50–56.

[11] J. Miller G3RUH, 9600 baud packet radio modem PCB, Issue 3, 1989.