Ideal Risk Avoidance and Survivability of Ultra Long Life Space Systems

Julian O. Blosiu
Avionic Systems and Technology Division
Jet Propulsion Laboratory/California Institute of Technology
Phone: (818) 354-1686/fax: (818) 393-4539
E-mail: Julian.O.Blosiu@jpl.nasa.gov

ABSTRACT

This paper describes the ideal space survivability of ultra long life systems (ULLS) in the context of ideality of risk avoidance. The psychology of risk vis-a-vis the opportunity to learn and gain new scientific knowledge of the universe is presented in general terms. Planning for risk management and performing systematic risk avoidance views risk as a positive learning opportunity. Levels of risk are determined by the degree of understanding functional requirements and performance requirements. Three levels of risk management zones are described; comfort, challenge, and excitement. Space event driven requirements are translated into the highest level of risk and are categorized as the excitement zone of risk management domain. Risk analysis, risk management, and risk free mitigation is considered as the first priority tasks to be performed for the ULLS. The nominated-up of risk avoidance and actions for risk mitigation creates the measurable attributes for the design decision criteria. Performance requirements of a given functional requirement are described as the nominated-up design option minimizing the allowable risk. For autonomous ULLS, model based autonomous risk management and risk seeding with test verification and validation are suggested as the practical approach for ULLS risk management and risk avoidance.

BACKGROUND

In the past, in order to reduce known risks to negligible levels, NASA space project implementations emphasized the maximization of fault tolerance practices to ensure mission success. Space projects such as Pioneer 10, Voyager 1 and Voyager 2 are living examples of space Ultra Long Life Systems (ULLS). Pioneer 10 was launched in 1972 and the two Voyager spacecraft were launched in 1977. Here we are in 2001 and all three spacecraft are still alive and ticking.

As NASA is embarking on establishing long duration interstellar missions, there is an urgent need to establish survival requirements for ULLS. When implemented the ULLS will survive for a minimum of 50 years or possibly 100 years. The flight time of a mission to Alpha Centaury (the closest solar system to our sun) might be shorten to 40 or 50 years by the most recent and promising breakthrough technology of light sail. The key element for ensuring survivability of ULLS, determines how to prevent and avoid catastrophic failure of evolvable, morphable, self healing, and event driven flight systems embedded in a highly autonomous and reliable spacecraft. Early risk management and planning by performing risk identification and risk avoidance is the answer to failure prevention. What is needed for ULLS is a general taxonomy [1] of risk categories and possible approaches to ideal risk avoidance.

OBJECTIVE

The main objective of this paper is to provide a general relationship between desired need of continuously advancing our knowledge of the universe, the ultra long life space systems and the total risk avoidance as the main condition for long life. The ideal [2] objective of a ULLS is to have an infinitely long life system. In other words, the system should live forever thus providing knew science knowledge forever. This implies that the system's risk of failures [3] should continuously and permanently be reduced to zero. Therefore, in the case of ULLS, the first and most important

requirements are the risk identification, risk management, and risk mitigation. The desired objective is to identify and categorize all levels of risk and the associated action to eliminate risk. The higher the level of risk, the more thorough the action for risk identification, mitigation, and avoidance should be. Expected life can only be increased by reduced risk, and the increase of risk induces a decrease in life.

PSYCHOLOGY OF RISK

It is well known that where there is no risk there is no growth. Thus, risk is not only associated with looking for opportunity, but also posed by uncertainty and failure [12]. If risk is viewed as a bad thing and a source of fear of not succeeding, people develop a natural defense mechanism such as setting up blinds and excuses for avoiding taking risk. In the long term, they deprive themselves of growth. The stronger the fear of risk and associated failure, the stronger the panic attacks on decision for action. Psychology at work [14][16] suggests that the normal positive approach is to view risk as a good thing and as an opportunity and a source of satisfaction that is there to be seized. When the blinds and excuses for actions are removed, the opportunity to grow and the potential accomplishment and satisfaction will replace the bad fear of failure with the good enjoyment of growth and realization. Lateral thinking [4] of thorough analysis of the possibilities for growth vis-à-vis risk avoidance is the process to be undertaken in identifying alternatives of design for action when embarking on any new endeavor. Identifying alternative ways for avoiding failure, in spite of potential risk, will instill confidence in seeing the light of success "at the end of the tunnel". Risk analysis can stimulate the search for opportunities in the context of calculated risks taking. Risk management is the vehicle that, when properly defined and applied, will substantiate the risk as a good and even enjoyable possibility stimulating the desire for action. Making mistakes and expecting calculated failures in a pre-planned safe environment of risk mitigation is what risk management is all about. In this context, risk is interpreted as a systematic search for new opportunities to learn new things that will provide potential rewarding results and growth. Thus, in psychological speaking terms, the risk management and mitigation planning activity becomes in itself an enjoyable practice to be expected and followed.

RISK MANAGEMENT PROCESS

The risk management process in general includes activities such as risk identification, analyses, planning, tracking, and control. The process for an ULLS begins with a thorough analysis an assessment of project constraints which determine the risk policies with respect to science objectives, mission life, mission success criteria, environmental factors, design decision options, technology readiness, safety issues, launch vehicle, development schedule, resources limits, legal, security, and liability.

Risk management a process to be continuously performed during the entire life cycle [11] of the project. It includes several required steps, such as: identification of all possible risks; analysis and prioritization of risk impacts; development of risk management plans; acceptance and/or rejection of risk mitigation; tracking risk and implementing mitigation plans; supporting timely and effective decisions to control risk; recording all facts in a history data base for future references; and ensuring that risk information is made available and communicated to all levels of risk management control. All risks should be disposed before delivery to operation.

In the case of ULLS autonomous projects, risk management activity should be autonomously performed making use of risk modeling and simulation with risk of faults and errors seeding techniques.

RISK MITIGATION AND LEVELS OF EVENT DRIVEN REQUIREMENTS

Three levels of risk categories are envisioned in establishing the planning and executing risk management and mitigation for ULLS. These levels are determined by the comprehensive knowledge available of the event relating to the functional and performance requirements to be implemented during the performance of a ULLS mission.

LEVEL I – The Comfort Zone. The first category is the situation when the event is known. **We know that we know the functional requirement,** and **we know that we know the performance requirement(s)** of the function to be performed. An ideal function is the function for which we have a complete detailed and exact knowledge of the functional and performance requirements. Thus, this is the situation where we are confident that "we know that we know" this function in all of its details. In this situation, risk mitigated design options are providing the most appropriate risk management and avoidance that can be performed with the classical risk management approach [5][6]. Level I category can be viewed as the comfort zone of risk management domain. This is the least difficult risk management planning and implementation level and is viewed as a surmountable risk management planning and risk avoidance activity. In this situation, only little or no on-board autonomous risk modeling and simulation is envisioned

LEVEL II – The Challenge Zone. This level of ULLS risk avoidance is an event driven situation, where we know that we do not know the event. When translated to requirements, **we know that we know the functional requirement,** but **we know that we do not know the performance requirements** of the given function. This is the mead-way to the ideal function requirement for which we only have a partial understanding of a function to be implemented. For this situation, we only believe we understand the functional requirement but little or no knowledge is available on the performance requirements. To be more specific, the parametric requirements are un-known and possibly are dictated by an event driven environment. In this case, much needs to be learned to fill the knowledge gap about the performance requirements and the associated risk mitigated design implementation. Onboard spacecraft modeling, simulation, test, and validation of the event driven performance requirements is the suggested approach to learn what are the most effective risk mitigated design options for the newly learned performance constraints. Techniques such as design of experiments, robust design/Taguchi methods [7], statistical process control and other heuristic techniques could be used for gaining the knowledge of the performance requirements. New design approaches and design decisions are needed to accommodate the spread of new performance requirements. To coup with the new challenges of the on-board design selection, a comprehensive on-board risk modeling and simulation is strongly suggested. On board autonomous risk assessment test verification and validation similarly to ground independent verification and validation [17] is also suggested. Methodologies for recognizing and avoiding errors in complex situations are strongly encouraged [1]. The category of risk in this case deals with a medium level of un-surmountable risk to be managed. Level II category is viewed as the challenge zone of risk management domain.

LEVEL III - The Excitement Zone. This is the situation where we have no a priori knowledge of a possible event to drive the functional and performance requirements in general. In this environment, **we do not know that we do not know the function to be performed**, and **we do not know that we do not know the actual parameters driving the performance requirements** of the un-known function. Contrasting to the ideal function, this is the situation where on the functional performance and requirements there is no knowledge whatsoever on what function is to be performed, let alone the performance requirements of the unknown function. This is identified as the event driven situation where " we do not even know what we do not know" the functions to be performed and the associated performance requirements for the new event. In order to accumulate new lessons learned that becomes knowledge of new functions and related performances, advanced and very sophisticated autonomous learning mechanisms are needed. Modeling, simulation, error seeding techniques, autonomous testing and validation, as well as Taguchi methods and other heuristic approaches are considered useful tools to be used. The response and adaptation of the ULLS to an event with a previously unknown function to be performed provides an un-surmountable risk level of the highest order. On the other hand, as stipulated above, the higher the risk, the higher the opportunity to gain more and exciting knowledge. In fact, this situation presents

the real opportunity to plow new ground and learn completely new knowledge. That is why Level III should be considered as the exciting zone of the risk management domain.

INTERDEPENENCE BETWEEN IDEAL ULLS AND IDEAL RISK AVOIDANCE

The ultimate objective of any space mission is to gain scientific knowledge of the universe, and in the long term to better our life here on Earth. As mentioned earlier, the objective of an ultra long life space system, as an ideal case, is to survive forever such as to be able to gather as much information and knowledge as possible. The survival length depends on the degree of avoiding risk of failure. In the case of ULLS, the Degree of Ideality of the ULLS (DIULLS) is directly proportional to the Degree of Ideality of Risk Avoidance (DIRA), or

$$DIULLS \cong DIRA.$$

On the other hand, when the number of un-recoverable failures approaches zero, the DIRA approaches infinite, or the ideal risk avoidance. This implies that the ideal risk avoidance is the situation when all risks of failures are continuously identified, mitigated and disposed. Therefore, the DIRA is inversely proportional to the sum of Un-Recoverable Failures ΣURF, or

$$DIRA \cong 1/\Sigma URF.$$

Also, in the case of an ULLS mission, the desire is to implement as many functional requirements (ΣFr) and performance requirements (ΣPr) as possible, or ΣFr + ΣPr. The sum of all Scientific Knowledge (ΣSK) gained is directly proportional to the number of successful functions implemented, or

$$\Sigma SK \cong (\Sigma Fr + \Sigma Pr).$$

In parallel, DIRA is also directly proportional to ΣSK. In other words, the higher the ideality of risk avoidance, the higher the payoff of scientific knowledge is. Doing all combinations and substitutions, DIULSS can be quantified and measured by using the following relationship:

$$DIULLS \cong (\Sigma Fr + \Sigma Pr)/\Sigma URF$$

This last relation, as stated, clearly demonstrates that the ideal ULLS is as much dependent on the functional and performance requirements implemented, as well as it is on the minimization of the un-recoverable faults. First, this last relation further strengthens the corroboration and inter-dependence between risk mitigation of faults, implement-ability of event driven requirements, and ultra long life systems. Second, taking a closer look at the above relation, it can be also observed that the real driver to reaching an ideal ULLS is the ability to reduce to zero the number of un-recoverable faults, and thus reducing the risk of faults to zero. When,

$$\Sigma URF \rightarrow 0 \text{ then, } DIULLS \rightarrow \infty$$

On the other hand, an increase of the number of event driven functional and performance requirements would definitely improve the degree of ideality of the ULLS, but would not push its value to infinity, unless there are an infinite number of implemented requirements considered.

RISK AVOIDANCE FIRST, DESIGN OPTIONS SECOND, IMPLEMENTABLE REQUIREMENTS THIRD.

In traditional systems implementation as shown in Figure 1, requirement specifications are considered first, design decision and implementation are second, followed by risk identification and avoidance as the third activity.

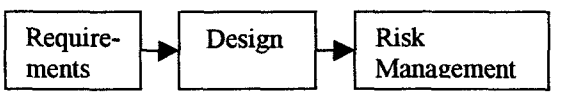

Figure 1. Traditional system implementation

Requirements, in general, are of two major categories [8]. First is the functional requirement category that specifies what function is to be performed. The second category includes all the performance requirements, which identify the numerical quantified performance parameters and associated constraints for the required function to be implemented. The implementation of a desired function could be accomplished by many different design options [13]. Each of these design options will implement the function by a different

design form. The form of each design implementing the desired function imprints different performance constraints. Thus, form has a direct relation to the design option selected to implement the function. The immediate conclusion is that in reality, form follows design option, more so than form follows function. Patterson and Evans [9][10] have suggested that in reality design decision for design option should in fact be considered first, as where performance requirements are fully known and understood only after implementing the design decision option. Following this logic, performance requirements are then placed as a far third from the functional requirement, a medium second from design decision, and a close first from the implemented design option. The "nominated-up" design options constitute the basis for finalizing the performance requirements that are driven up by the measurable attributes of the implemented outcome of the design decision. Figure 2 illustrates this concept.

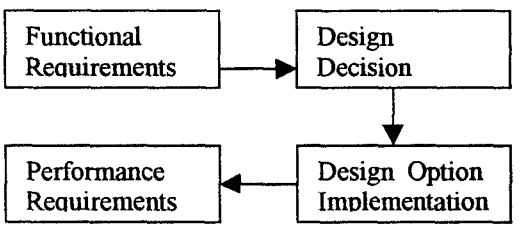

Figure 2. Design decision and implementation before performance requirements.

In the case of ULLS, the long life of a system is directly proportional to risk mitigation. Risk avoidance includes all of the mandatory steps that will prevent loss of space system resources. These resources include time, cost, material goods, energy, power, scientific knowledge, lessons learned, and the ULLS spacecraft is the ultimate resource. Thus, risk mitigation and avoidance should be considered the first step as the guiding criteria for survival of an ultra long life space mission.

Implementation form of each design decision option presents different kinds of risks and risks levels. The process starts with an originally thought functional requirements. In the event driven spacecraft environment, the event determines the functions to be performed. The performance requirements to be implemented would largely depend on the risk free design decision selected. For this reason, risk mitigation and avoidance is best addressed in the design approach and the design decision to be made. All of the constraints imposed by the risk mitigation and the avoidance of loss of resources will provide the criteria for selection of the mitigated risk or possible risk free design option. The "nominating-up" of risk avoidance and actions for risk mitigation will create the measurable attributes for the decision design criteria for hardware, software, and process options. It becomes obvious that for the ULLS, design decision and design option selected becomes the second activity step to be performed.

In turn as a third step, for a given original functional requirement, only the performance of a desired function that is leading to risk free design performance will be allowed to be considered for implementation. Performance requirements are in fact driven by the nominated-up design option that would minimize the allowable risk, and not the other way around. As an ultimate conclusion, to ensure survivability of ULLS, only functions and performances that are implemented by risk free designs are aloud to be considered for implementation. Figure 3 describes this concept.

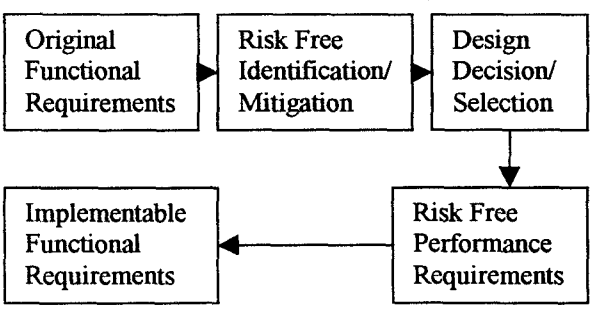

Figure 3. Risk-free first, design decision second, performance third, function fourth.

MODEL BASED RISK MANAGEMENT AND RISK SEEDING

As described above, for long life space systems, on board autonomous risk identification, mitigation, and management become the first priority for consideration. In the traditional reliability assurance technique, redundancy is performed by duplicating components by function. Since

both components could fail, other innovative techniques are suggested, such as self-healing and polymorphism. Self-healing technique repairs components that failed. Polymorphism technique uses generic architectural blocks that could perform more than one function. These last two techniques are emerging as new technology thrusts including such new technologies as evolvable hardware, software, and systems. An important characteristic of the ULLS is to be able to self evaluate and mitigate risks for all situations and risk categories. In the situation of an event driven space mission, on-board autonomous risk modeling is one of the suggested viable approaches to be considered [15]. Earlier, we identified different levels of risks such as dealing with surmountable and un-surmountable risk categories. This implies that depending on the category and level of risk, different categories of risk seeding are to be used, for risk modeling. Risk modeling using risk seeding techniques are used to simulate event driven conditions where knowledge of risk avoidance is needed to be learned and applied in the design implementation of the event driven function. The type and depth of risk seeding will depend on the three previously identified risk categories, such as: modeling with surmountable risk; modeling with un-surmountable risk; and modeling with an intermediate level of un-surmountable risk. As the adaptive/evolvable hardware and software technologies are maturing, the process of on-boar risk autonomous modeling by using risk seeding techniques is becoming very attractive. For each of the three categories of risk modeling the difference will rely on the depth and extent of the risk modeling and the extent of risk seeding approach.

CONCLUSION

Only in a total fault avoidance environment the long life of a ULLS is ascertained. The ideal ULLS is to live forever. The ideal risk avoidance is to prevent all faults. Risk mitigation actions are: a) empowered by evaluating possible risks and determining level of risks, b) nourished by risk avoidance options, and c) realized by validation data and factual elimination of all faults. For ULLS, risk is first, risk free design decision and design option are second, and allowable performance requirements for a given function are third

.

AKNOWLEDGEMENT

The work described here was performed at Jet Propulsion Laboratory/California Institute of Technology under a contract with the National Aeronautics and Space Administration

REFERENCES

[8] Andriole,S.J., "Managing Systems Requirements: Methods, Tools, and Cases", McGraw-Hill, 1996, USA

[2] Blosiu, J. O. and Blosiu, C. J., "Perfection, Ideality, and Technology Road Map as Measured by a Sliding Scale (*Technology Creativity metrics)*", IEEE International Conference on Management of Innovation and Technology, pp. 321-326, 12-15 November, 2000, Singapore.

[7] Blosiu, J. O., Deligiannis, F. and DiStefano, S., "NiCd Battery Optimization Using Taguchi Methods," ASI 2-nd Annual Total Product Development Symposium, November 6-8, 1996, Pomona, CA. USA.

[17] Blosiu, O. J., "Independent Verification and Validation of Computer Software: Methodology," Jet Propulsion Laboratory Document (JPL D- 576), 198, USA.

[1] Carr, M. J., at all, "Taxonomy-Based Risk Identification, Technical Report CMU/SEI – 93-TR-6, ESC-TR-93-183, Software Engineering Institute, CMU, USA.

[3] Dorner, D., "The Logic of Failure", Metropolitan Books, 1996, USA

[4] de Bono, E., "Later Thinking", Harper and Row, Publishers, 1970, USA.

[9] Evans, R.P, Park, S. and Albert, H. "Decision Not Requirements," in Proceedings, IEEE Computer Society Conference on the Engineering of Computer-Based Systems, Los Alamitos, California, USA: IEEE Computer Society Press, 1996, pp. 55-59.

[16] Fischoff, B., Slovic, P. and Lichtenstein, S., "Fault Trees: Sensitivity of Estimated Failure Probabilistic to Problem Presentation," Journal of Experimental Psychology: Human Perception and Performance, pp. 330-334, 1078

[14] Kahneman, D. and Tversky, A., "On the Psychology of Prediction," Psychological Review, pp. 237-251, 1973, USA

[15] Klein, H. J., "Modeling Risk trade-off" Journal of Operational Research Society, pp. 445-460, 1993, USA

[13] Moore, G. P. and Thomas, H., "Anatomy of Decision," London: Penguin Book, 1976, UK

[6] NASA Program Procedures and Guidelines, NPG: 7120.5A, 03-03-1998, USA

[10] Patterson F.G. Jr. and Evans, R. P., "Perfecting the Image," in Proceedings of the 1998 IEEE International Conference on Systems, Man, and Cybernetics: Intelligent Systems for Humans in a Cyberworld. DiCesare, F., and Jafari, M. A., Editors, Los Alamitos, California, USA: IEEE Computer Society Press, 1998, pp. 2709. Also appeared in Proceedings, 1999 NASA Great Authors' Colloquium, Hagerstown, Maryland, USA.

[5] Rose, J., "Risk Management Handbook for JPL Projects – D-15951t", October 1, 1998, JPL, USA

[11] Wards, S.C. and Chapman, C. B., "Risk Management and the Project Life Cycle", International Journal of Project Management, pp.145-149, 1995

[12] Weldeman, M., "Project and Program Management: A Guide to Managing Project Risk and Opportunities", The PMBOK Handbook Series- Volume 6, P.O. Box 43, Drexell Hill PA, 19026-0043, USA.