

On-Board Preventive Maintenance for Long-Life Deep-Space Missions: A Model-Based Analysis*

Ann T. Tai
IA Tech, Inc.
10501 Kinnard Avenue
Los Angeles, CA 90024

Leon Alkalai Savio N. Chau
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, CA 91109

Abstract

The long-life deep-space missions associated with NASA's X2000 Advanced Flight Systems Program creates many unprecedented challenges. In particular, the stringent constraints on the mass of a spacecraft and the power on-board preclude traditional fault tolerance approaches which rely on extensive component/subsystem replication, calling for novel approaches to mission reliability enhancement. In this paper, we present an approach to on-board preventive maintenance which rejuvenates a system via periodical duty switching between system components, slowing down a system's aging process and enhancing mission reliability. By exploiting the nondedicated system redundancy, hardware and software rejuvenation are realized simultaneously without significant performance penalty. Our model-based evaluation confirms a potential for significant gains in mission reliability from on-board preventive maintenance and provides to us useful insights about the collective effect of age-dependent failure behavior, residual mission life, risk of unsuccessful maintenance and maintenance frequency on mission reliability.

1 Introduction

With NASA's spectacular return to Mars on July 4th, 1997, the Mars Pathfinder Lander and its Sojourner Microrover have set a new standard for *Faster, Better, Cheaper* space exploration missions. X2000, a new-generation space technology program aimed at providing an engineering model to multiple long-life deep-space missions [1, 2], is intended to realize the new standard by achieving at least an order of magnitude improvement in both performance and dependability under stringent power and mass constraints. Further, the X2000 technology will enable a high-level efficiency that the cost of the multi-mission purpose spacecraft could be lower than that of the Mars Pathfinder spacecraft. Currently, five missions are designated to be the receipts of the X2000 technology: Europa Orbiter, Pluto-Kuiper Express, Solar Probe, Mars Sample Return and DS4/Champion (also known as Comet Sample Return). Thus, X2000 will supply benchmarks for NASA's new standard.

With respect to the X2000 missions, reliability implies a system's continuous operation up to 15 years and availability is the system's readiness to service a mission in an unknown deep-space,

radiation intense environment. In order to simultaneously meet the power, mass and dependability criteria, the X2000 system architecture employs adaptive fault tolerance techniques that exploit nondedicated system redundancy. To further enhance mission reliability, we have been investigating into the notion of *on-board preventive maintenance* [3]. By "on-board preventive maintenance," we mean the actions taken place during a mission for eliminating or minimizing potential error conditions that accrue over the operational life of a spaceborne system. Although the concept is analogous to that of "software rejuvenation" which has received an appreciable amount of attention in the past few years [4, 5, 6], on-board preventive maintenance concerns both hardware and software and must be realized in a manner which keeps the maintenance-caused unavailability minimal. Specifically, from software perspective, aging phenomenon such as memory leakage and data corruption can be removed via program reinitialization which cleans up a system's internal state [4] (complete age reversal); from hardware perspective, the effects of electron-migration (the driving force of circuit failures), which occurs in microelectronic devices when current density is high, can be reduced through structural/thermal relaxation during a power-off period [7, 8] (partial age reversal). Accordingly, the procedure of on-board preventive maintenance for the X2000 spaceborne computing system involves 1) stopping the running software and host hardware system, and 2) rebooting the system and restarting software execution after a scheduled time interval. To minimize maintenance-caused system unavailability, we exploit nondedicated system redundancy. An instance of nondedicated redundancy in the X2000 computing system is the following: During a critical mission phase which demands a full computation power (such as the Encountering Phase in the 15-year long Pluto-Kuiper Express mission), all the processor strings are scheduled to jointly perform the spacecraft and scientific functions, while only a subset of the strings is mandated to be in service during less-critical mission phases such as a cruise phase. Hence, individual processor strings can rotate between on-duty and off-duty shifts based on a scheduled time interval, we call it a *duty period*, for preventive maintenance throughout the mission except during the phase(s) requiring a full computation power. In this manner, on-board preventive maintenance practically has no negative effect on system availability.

In order to study optimal maintenance frequencies that balance the risk of system failure due to component aging against that due to unsuccessful maintenance, we have conducted model-based

*The research described in this paper was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

analyses. Our initial study [3] demonstrated the feasibility of on-board preventive maintenance. For simplicity, the analysis was based on the assumption that the aging processes of hardware and software components both could be completely reversed through preventive maintenance and thus could be treated the same in analytic evaluation. Although this assumption sufficed the purpose of our preliminary study, we have been investigating into this subject in further depth by discriminating between the aging, age-reversal and failure behavior of hardware and those of software. To accomplish the objective, we use Weibull distribution to characterize system component's aging and age-reversal processes in a cohesive manner. We then derive a recursive function for mission reliability evaluation which captures the dependencies of system components' aging/failure behavior between duty periods. Further, we extend our basic model to facilitate phased-mission analyses. Inspired by the results of our earlier study which revealed that optimal duty period is operational environment dependent [3], we utilize the extended model and the mission profiles of Pluto-Kuiper Express and DS4/Champlion to investigate into the influence of adjusting duty period to mission phases on reliability gain. The evaluation results confirm a potential for significant gains in mission reliability from on-board preventive maintenance and provide to us useful insights about the collective effect of age-dependent failure behavior, residual mission life, risk of unsuccessful maintenance and maintenance frequency on mission reliability.

The remainder of the paper is organized as follows. Section 2 provides the background information about the X2000 system architecture. Section 3 describes the method of model construction, followed by Section 4 which discusses the results of the analytic evaluation based on two X2000 mission profiles. The concluding section summarizes what we have accomplished and discusses our plan for future research.

2 Background

One of the major challenges the X2000 program exhibits to us is the requirements diversity among the five missions, which demand a computation power from a single processor string to multiple strings, a throughput range from under 20 MIPS to over 100 MIPS, and a mass memory size from 100 Mbytes to 1.5 Gbytes. Therefore, the X2000's computing system architecture must be scalable and distributed in order to accommodate a broad spectrum of requirements. As far as the avionics concern, the X2000 is aimed at further advancing the packaging technologies initiated by the New Millennium Deep Space One (NMP DS1) program [9, 10]. The NMP DS1 developed an architecture which consists of a RAD-6000 processor multi-chip-module (MCM), a local memory MCM, a non-volatile mass memory MCM, and an I/O MCM. The X2000 architecture has taken a further step toward miniaturization, in which each processor string consists of a processor slice integrated with I/O interfaces, a local memory slice, and one to four non-volatile mass memory. Moreover, the X2000 architecture has been extended through employing multiple processor strings connected by redundant buses, namely, IEEE 1394 and I2C, to enhance mission reliability and performance [11]. As the use of standard buses enables the X2000 architecture to be scalable, the system can accommodate from one to multiple processor strings. An instance of a two-string configuration of the X2000

architecture is depicted in Figure 1.

A main feature of the X2000 system architecture is the I/O cross-strapping for the processor strings that is implemented using the standard interfaces of IEEE 1394 and I2C. This feature permits the workload that comprises the spacecraft and science functions to be shared by and migrated between processor strings in an efficient manner. Therefore, the I/O cross-strapping plays an important role in enabling adaptive utilization of system resource redundancies, a cost-effective way to the realization of dependability and performance enhancement. Among other things, on-board preventive maintenance schemes have been proposed to take advantage of this feature. That is, during less critical mission phases such as cruise phases, the processor strings will be scheduled on and off duty periodically, servicing the mission on a rotation basis. The benefit from this approach is two-fold: 1) a significant saving for the limited power on-board, and 2) periodic rejuvenation for both hardware and software of the processor strings.

3 Methods of Model Construction

3.1 Problem Description

The analytic models we develop in this section are based on the system configuration of the X2000 architecture with two processor strings. We first construct a basic model that captures the essence of on-board preventive maintenance; we then extend the basic model for phased-mission analyses. Based on the extended model, we investigate into the preventive maintenance strategies using the mission profile of Pluto-Kuiper Express which is to explore the unsurveyed planet Pluto and Kuiper Disk. As Pluto is the most distant planet in the Solar system, this mission will travel the greatest distance from Earth and have the longest duration among the X2000 missions (15 years). We carry out further investigation based on the profile of DS4/Champlion which is a sampling-return mission.

Due to the combined consideration of the time-increasing failure rate and partial age reversal, we face a challenge of representing the dependencies between duty periods. In particular, when a new duty period begins, the age of the string which just completes its maintenance and becomes power-on again is a function of 1) the accumulated amount of time comprising the lengths of the duty periods the string has serviced since the mission starts, and 2) the amount of age reversal it has obtained from the prior preventive maintenance. Another difficulty in model construction arises from the fact that the continuation of the duty-switching sequence will depend upon the availability of resource redundancy. Specifically, resource redundancy may become temporarily or permanently unavailable for preventive maintenance if both strings are required to jointly service the mission or one of the strings fails, respectively. Moreover, the simultaneous consideration of hardware and software rejuvenation requires us to 1) differentiate their aging, age-reversal and failure behavior, and 2) capture the interactions between hardware and software. Finally, analyzing phase-adjusted on-board preventive maintenance needs us to deal with a "phase hierarchy" in the sense that each *duty period* can be viewed as a mission phase at the lower level while each actual *mission phase* at the higher level consists of duty periods. Although various approaches to phased-mission analysis were proposed by other researchers (see [12, 13, 14], for example), analytic models

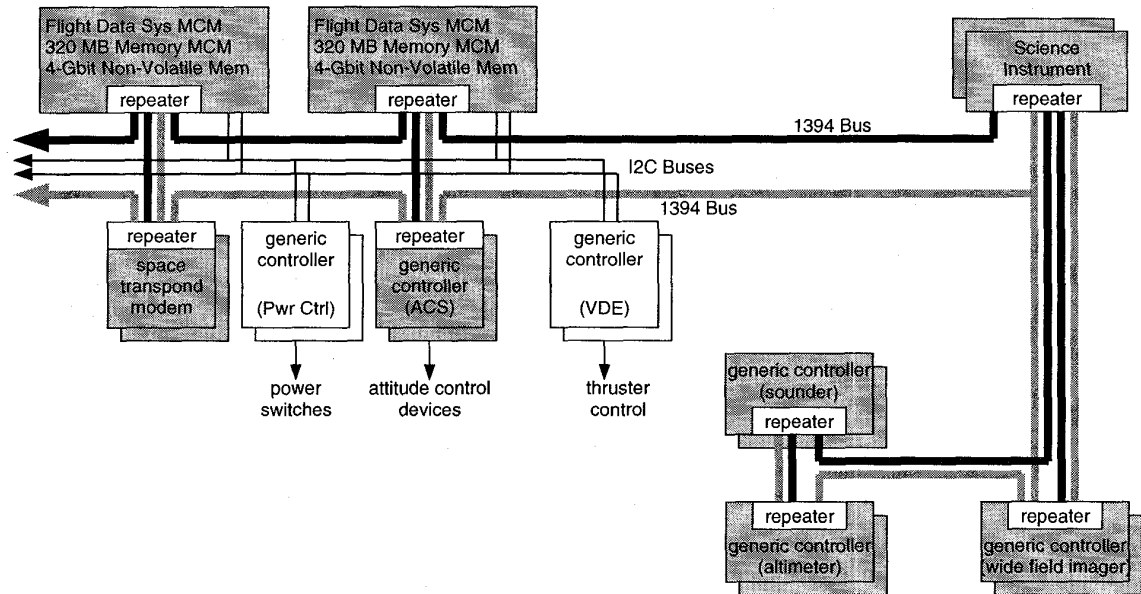


Figure 1: X2000 System Architecture

considering the requirements described above have not yet been investigated. In the subsections that follow, we develop a model construction method in which

1. Weibull distribution is utilized to characterize a system component's aging and age-reversal behavior in a cohesive manner.
2. A recursive function is derived to facilitate the representation of the dependencies between duty periods, with respect to the aging, age-reversal and failure behavior of system components.

Before we proceed to describe the model construction method in further detail, we explain our assumptions as follows.

- 1) In accordance with the theory that power-off periods will improve a microelectronic device's lifetime [7], we postulate that the amount of age reversal obtained by the hardware of a string through preventive maintenance is directly proportional to the amount of time during which a string undergoes preventive maintenance (which equals to the length of a duty period due to the rotation-based maintenance scheduling).
- 2) Both hardware and software failures considered in the model are permanent in nature and will cause the corresponding string to be in a non-operational state. Upon the failure of one of the strings, the surviving one will attempt to take over the workload. However, if both strings fail, the computing system will become non-operational, which leads to an unsuccessful mission.
- 3) A string may crash when it attempts to takeover the workload from its peer during scheduled duty switching or during failure recovery, causing the system to be in a non-operational state. We call this event "an unsuccessful duty switching"

and use the term "switching coverage" to refer to the complement of the probability of such an event.

- 4) A string will not fail during its power-off periods.

3.2 Characterizing Aging and Age-Reversal Processes with Weibull Distribution

The Weibull distribution is the most commonly used distribution in reliability engineering because by a proper choice of its shape parameter, an increasing, decreasing or constant failure rate distribution can be obtained [15]. Weibull distribution has been used to describe system behavior with time-increasing failure rate such as fatigue failure, vacuum-tube failure, etc. In fact, Weibull distribution not only enables us to characterize the age-dependent failure rate of a system component by properly setting the shape parameter but also allows us to model the age-reversal effect from on-board preventive maintenance through the use of the "location parameter." Specifically, we can begin model construction with choosing the following form of Weibull probability density function [15]:

$$f(t) = \beta\lambda((t - \gamma)\lambda)^{\beta-1} e^{-((t-\gamma)\lambda)^\beta} \quad (1)$$

where β is the shape parameter (we set it to a value greater than 1 to represent the age-increasing failure rate), λ is the scale parameter and γ is the location parameter that defines the "origin" where the system begins to age and to have a potential for failure. To aid a more precise description, we depict a duty-switching sequence in Figure 2 and define the following notation:

- S The *service age* of a system component.
- δ The amount of age reversal resulting from a preventive maintenance.

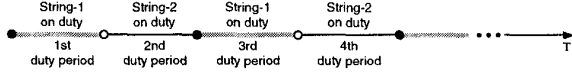


Figure 2: Duty-Switching Sequence

By “service age,” we mean the accrued amount of time during which a processor string is on duty to perform the spacecraft and science functions. As shown in Figure 2, the shaded regions will contribute to the service age of String-1. In these terms, the mathematical concepts for the aging and partial age-reversal processes of a *single* string can be illustrated by Figure 3. In the figure, the abscissa marks the service age of the string while the ordinate measures $h_i(S)$, its Weibull failure rate (hazard rate) function for the i th duty period, namely,

$$h_i(S) = \beta\lambda((S - \gamma_i)\lambda)^{\beta-1}$$

where γ_i equals to the quantity of partial age reversal accrued through the preventive maintenance prior to the i th duty period. Consequently, the term $(S - \gamma_i)$ in the above equation represents the “effective age” of a string in the i th duty period. For clarity of illustration, the shape parameter β is set to 2 such that $h_i(S)$ is linearly increasing within the i th duty period. The solid dots mark the beginning of each duty period for the string (presuming that a duty period has a duration of 10 weeks in this example). The lines with arrows at their right hand sides illustrate the effect of partial age reversal from preventive maintenance. More precisely, these lines indicate the following: By the time when the string is ready to start a new duty period, its age has been reversed, due to the effect of the preventive maintenance just completed, by δ time units (assuming 5 weeks in this example) as if its “birthday” (which is represented by the value of the location parameter γ_i) moves forward along the service-age horizon (such that it becomes “younger”). Each thick solid line represents the effective failure rate of the string for a particular duty period. Finally, each dashed line with arrows at both ends measures the effective age of the string at the time when it starts a new duty period.

3.3 Capturing Dependencies between Duty Periods with a Recursive Function

3.3.1 Basic Model

The system’s behavior with respect to duty periods is a regenerative renewal process [16], which can be translated into a duty-period oriented timing diagram shown in Figure 4. The notation used in the figure are defined below:

- θ The duration of a mission life.
- n The number of duty periods in a mission.
- ϕ The duration of a duty period.
- k The number of duty periods with successful completions prior to the first string failure.
- x The service age of a string’s hardware at the time when its error condition causes the first string failure.

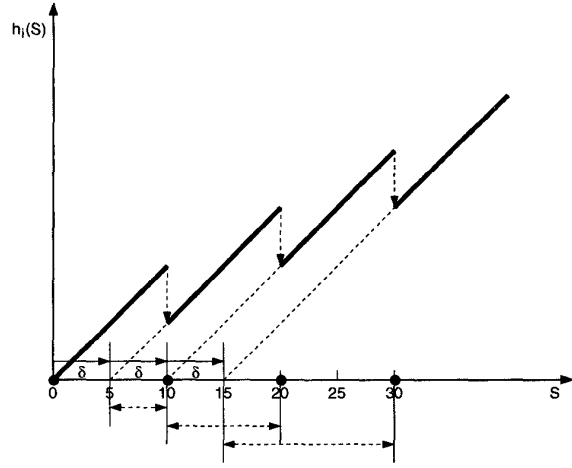


Figure 3: Partial Age-Reversal Concept from Service-Age Perspective

- y The service age of a string’s hardware at the time when its error condition causes the second string failure.
- u The service age of a string’s software at the time when its error condition causes the first string failure.
- v The service age of a string’s software at the time when its error condition causes the second string failure.

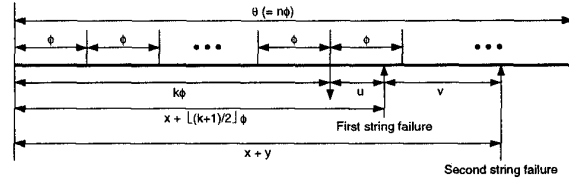


Figure 4: Duty-Period Oriented Timing Diagram

The timing diagram illustrates the success and failure scenarios in terms of duty period and service ages of hardware and software, and describes the relationships between them. Namely,

- 1) $k\phi$ marks the first k duty periods during which both strings do not fail.
- 2) $x + \lfloor \frac{k+1}{2} \rfloor \phi$ (or interchangeably, $k\phi + u$) is the time to the first string failure due to a hardware or software error, where x and $\lfloor \frac{k+1}{2} \rfloor \phi$ are the service ages of the failed and surviving strings at the time of the failure, respectively.
- 3) $x + y$ (or interchangeably, $k\phi + u + v$) is the time to the second string failure due to a hardware or software error.

Based on the timing diagram, we can analyze the system’s success and failure scenarios:

- S1: $k = n \Rightarrow$ Both strings do not fail during the mission.
- S2: $(k < n) \wedge (x+y > n\phi) \Rightarrow$ The first string failure occurs during the $(k+1)$ th duty period due to a hardware or software error and the surviving string remains operational through the remainder of the mission.
- S3: $(k < n) \wedge (x+y \leq n\phi) \Rightarrow$ The first string failure occurs during the $(k+1)$ th duty period due to a hardware or software error and the surviving string subsequently fails before the end of the mission.

Let $R(\theta)$ denote the reliability of a mission with duration θ , clearly

$$R(\theta) = P[S1] + P[S2] \quad (2)$$

Before we proceed to derive the solution for $R(\theta)$, we introduce the following notation

- $T_1[i]$ The service age of a string's hardware at the time when the string starts its duty for the i th duty period.
- $T_2[i]$ The service age of a string's hardware at the time when the string completes its duty for the i th duty period.

From the diagram that illustrates the duty-switching sequence (Figure 2), it follows that,

$$T_1[i] = \left\lfloor \frac{i-1}{2} \right\rfloor \phi, \quad T_2[i] = \left(\left\lfloor \frac{i-1}{2} \right\rfloor + 1 \right) \phi$$

We can then define $F[i]$ as the probability that a string fails during the i th duty period due to a hardware error, namely,

$$F[i] = \int_{T_1[i]}^{T_2[i]} f_i(x) dx \quad (3)$$

where f_i is the Weibull probability density function characterizing hardware's failure behavior in the i th duty period, that is,

$$f_i(t) = \beta\lambda ((t - \gamma_i)\lambda)^{\beta-1} e^{-((t-\gamma_i)\lambda)^\beta} \quad (4)$$

where $\gamma_i = \left\lfloor \frac{i-1}{2} \right\rfloor \delta$. And in accordance with the assumption that the amount of age reversal obtained by the hardware of a string through a preventive maintenance is directly proportional to the length of a duty period, we let $\delta = \rho\phi$, where the coefficient ρ has a domain $[0, 1)$.

Further, let $G[i]$ denote the conditional probability that a string fails due to a hardware error during the i th duty period given that both strings do not fail by the end of the $(i-1)$ th duty period. $G[i]$ can be solved in terms of a recursive function that facilitates the representation of the dependencies between duty periods, with respect to strings' aging, age-reversal and failure behavior. More precisely,

$$G[i] = \frac{F[i]}{\prod_{j=1}^{i-1} (1 - G[j])}, \quad i \geq 2 \quad (5)$$

with

$$G[1] = F[1]$$

Although there are alternative ways to formulate $R(\theta)$, we choose to employ the recursive function because it is easy to understand and facilitates model extension (as described in the next section). Based on $G[i]$, the first term in Equation (2) can be evaluated by a product-form expression,

$$P[S1] = c^{n-1} \prod_{i=1}^n (1 - G[i])(1 - Q[i]) \quad (6)$$

where c is the "switching coverage" (see Section 3.1) and $Q[i]$ is the probability that a string fails due to a software error during the i th duty period. Since software is able to obtain a complete age reversal through rejuvenation, the formulation for $Q[i]$ is simpler:

$$Q[i] = \int_0^\phi \hat{f}(t) dt \quad (7)$$

where \hat{f} is the Weibull probability density function with the shape parameter α and scale parameter μ that characterizes software's failure behavior:

$$\hat{f}(t) = \int_0^\phi \alpha\mu(t\mu)^{\alpha-1} e^{-(t\mu)^\alpha} dt$$

The derivation for the solution of the second term in Equation (2) requires us to consider the interactions between hardware and software failure behavior. To aid the formulation, we introduce the following notation:

- A_i The event that both strings do not fail by the end of the i th duty period.
- B_i The event that a string failure which is due to a hardware error occurs during the i th duty period and the surviving string remains operational through the remainder of the mission.
- C_i The event that a string failure which is due to a software error occurs during the i th duty period and the surviving string remains operational through the remainder of the mission.

Finally, we let

$$\begin{aligned} H[k] &= P[A_k \cap B_{k+1}] = P[A_k] P[B_{k+1} | A_k] \\ S[k] &= P[A_k \cap C_{k+1}] = P[A_k] P[C_{k+1} | A_k] \end{aligned}$$

According to its definition, $P[A_k]$ can be expressed as

$$P[A_k] = c^{k-1} \prod_{i=1}^k (1 - G[i])(1 - Q[i])$$

Based on the information supplied by the duty-period oriented timing diagram (Figure 4), the solutions for $P[B_{k+1} | A_k]$ and $P[C_{k+1} | A_k]$ can be obtained by analyzing the strings' service ages and residual mission life at the time of failure. Due to space limitation, the detailed explanation is omitted here but the resulting expressions for $P[B_{k+1} | A_k]$ and $P[C_{k+1} | A_k]$ are given in Appendix A (Equations (10) and (11), respectively).

To this end, the second term of Equation (2) can be given by

$$\begin{aligned}
P[S2] &= \sum_{k=0}^{n-1} c(H[k] + S[k]) \\
&= \sum_{k=0}^{n-1} c P[A_k] (P[B_{k+1} | A_k] + P[C_{k+1} | A_k]) \quad (8)
\end{aligned}$$

In turn, the measure we seek to evaluate, $R(\theta)$, can then be solved analytically.

3.3.2 Phased-Mission Analysis

Now we extend our basic model described in the previous section for a phased-mission analysis. The Pluto-Kuiper Express consists of three phases, namely, the Cruise Phase, Encountering Phase and Kuiper-Disk Exploration Phase, as shown in Figure 5, with phase durations of 12 years, 4 months and 3 years, respectively. Among the three phases, the Encountering Phase during which the spacecraft flies by Pluto is clearly the most critical to the mission. The crucial spacecraft functions include orbit maneuver and pointing; while those intensive scientific functions encompass taking high-resolution visible and infrared images, uplinking radio science phase shift data and storing them on-board for later transmission. Therefore, as mentioned previously, both strings will be powered on to perform spacecraft and science functions in this phase. After encountering Pluto, the mission enters the Kuiper-Disk Exploration Phase during which the spacecraft will attempt to encounter one or more Kuiper Disk objects as it continues its journey out into interstellar space. This phase is aimed at enabling the long-life mission to gain potential bonus. Due to this nature, the Kuiper-Disk Exploration Phase does not mandate a full computation power. Accordingly, on-board preventive maintenance will be allowed to resume during this final phase.

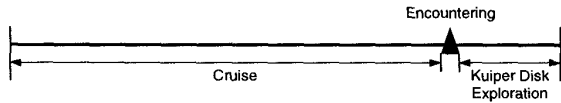


Figure 5: Mission Phases of Pluto-Kuiper Express

The notation used in describing the phased-mission analysis is defined below:

- n_1 The number of duty periods in the Cruise Phase.
- n_2 The number of duty periods in the Kuiper-Disk Exploration Phase.
- ϕ_1 The duration of a duty period in the Cruise Phase.
- ϕ_2 The duration of a duty period in the Kuiper-Disk Exploration Phase.
- Φ The duration of the Encountering Phase.
- δ_1 The amount of age reversal a string obtains from a preventive maintenance in the Cruise Phase.
- δ_2 The amount of age reversal a string obtains from a preventive maintenance in the Kuiper-Disk Exploration Phase.

If further, we let θ_1 and θ_2 denote the durations of the Cruise Phase and Kuiper-Disk Exploration Phase, respectively, then

$$\phi_1 = \frac{\theta_1}{n_1}, \quad \phi_2 = \frac{\theta_2}{n_2} \quad \text{and} \quad \delta_1 = \rho\phi_1, \quad \delta_2 = \rho\phi_2$$

where $\rho \in [0, 1)$.

The fact that the Encountering Phase requires both strings to be in service implies that preventive maintenance will temporarily halt. Therefore, special treatment is required for that particular phase. To preserve the generality of the equations developed for the basic model described in the previous section, we view the Encountering Phase as a special phase which can be “unfold” to become two “parallel” duty periods. More precisely, at the lower level of the model where strings’ aging and failure behavior are represented, we treat the parallel duty periods as two individual duty periods; on the other hand, at the high level where mission reliability is formulated, we view them as a single duty period. In this manner, the basic model for solving $R(\theta)$ can be adapted to accommodate phased-mission analyses with some minor modifications. First, we re-formulate γ_i , $T_1[i]$ and $T_2[i]$ by considering the parities of n_1 and i , and their relationships with the strings’ duty-switching scheduling (see Equations (12), (13) and (14), respectively, in Appendix A).

Based on the modifications, Equation (5) can be adapted to facilitate a phased-mission analysis by adding just one more boundary condition that is derived for handling the Encountering Phase which comprises two “parallel” duty periods:

$$G[i] = \frac{F[i]}{\prod_{j=1}^{i-1} (1 - G[j])}, \quad i \geq 2, i \neq n_1 + 1 \quad (9)$$

with

$$G[n_1 + 1] = \sum_{i=n_1+1}^{n_1+2} \frac{F[i]}{\prod_{j=1}^{n_1} (1 - G[j])}$$

and

$$G[1] = F[1]$$

Letting $n = n_1 + n_2 + 1$, reliability of the Pluto-Kuiper Express mission can then be evaluated using Equations (2), (6) and (8).

4 Evaluation and Discussion

Applying the model developed in the previous section and using *Mathematica*TM, the effectiveness of on-board preventive maintenance is evaluated based on the mission profile of Pluto-Kuiper Express. It is worth to note that the recursive function $G[i]$ and conditional expressions for $T_1[i]$ and $T_2[i]$ in the model can easily lend themselves to efficient computer manipulation by utilizing the built-in recursion capability and conditional constructs of *Mathematica*TM. First, we study the influence from the strategy of adjusting maintenance frequency to mission phase change on reliability gain. That is, mission reliability $R(\theta)$ is evaluated along two dimensions — against varying maintenance frequencies for the Cruise Phase and Kuiper-Disk Exploration Phase (n_1 and n_2 , respectively). The value assignment for other parameters is shown in Table 1 (in Appendix B), where all the parameters involving time (durations, rates, etc.) presume that time is quantified in weeks.

Table 2 (in Appendix B) displays mission reliability $R(\theta)$ as a function of n_1 and n_2 , where $R_0(\theta)$ denotes the “baseline mission reliability” — assuming the system does not have preventive maintenance during the entire mission. And Figure 6 provides a graphical presentation of the evaluation results, where n_1 and n_2 are plotted in a logarithmic scale. These illustrations confirm a potential for significant gains in mission reliability from on-board preventive maintenance, namely, an improvement up to two orders of magnitude relative to the baseline reliability can be accomplished. On the other hand, the evaluation reveals that extremely high maintenance frequencies will not be effective for mission reliability enhancement, as indicated by the entries of the row and column where $n_1 = 1000$ and $n_2 = 1000$, respectively. This can be understood by considering the tradeoffs between system component reliability improvement due to preventive maintenance and the likelihood of system failure caused by unsuccessful duty switching. In particular, an extremely high maintenance frequency will lead to excessive risk of unsuccessful duty switching which negates the benefit from preventive maintenance.

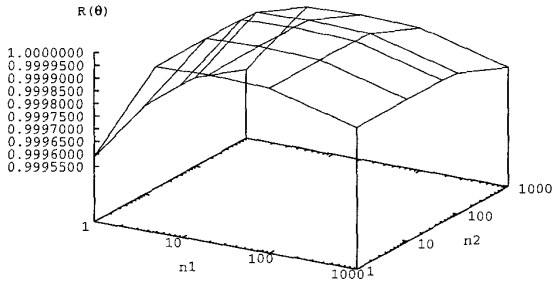


Figure 6: $R(\theta)$ as a Function of n_1 and n_2

A more interesting observation with regard to adjusting maintenance frequency to mission phase is the following: Intuitively, a later mission phase favors more frequent maintenance (thus shorter duty periods) due to a higher vulnerability of system failure derived from component aging. Contrarily, our evaluation results reveal that it will not be beneficial in general to increase maintenance frequency (i.e., to decrease the duration of a duty period) in the later mission life. Indeed, a strategy that exercises preventive maintenance in a less frequent manner in the later mission life will usually lead to an optimal mission reliability. As indicated by Table 2, for the particular mission in question, the optimal mission reliability will be achieved when $n_1 = 20$ and $n_2 = 1$, corresponding to the duty periods of 31.2 weeks and 156 weeks, respectively. In other words, the evaluation results suggest to us that not to resume preventive maintenance after the Encountering Phase will indeed benefit mission reliability. This surprising result stems from some tradeoffs among system attributes which may not be obvious without analytic modeling. Specifically, the likelihood that the system fails before the mission completion tends to 1) increase as the age-dependent failure rates of system components

increase, and 2) decrease as the residual mission life decreases. In other words, while the system becomes more vulnerable to failure as its components are aging, the decreasing residual mission life favors less frequent maintenance because the reliability improvement becomes less significant and may turn to be unable to compensate the risk of mission failure caused by unsuccessful duty switching.

Next we analyze the effect of switching coverage on optimal preventive maintenance frequency by using the set of parameter values shown in Table 1 but increasing the switching coverage c to 0.99999999. The evaluation results are displayed in Table 3 (in Appendix B). Contrast this table with Table 2, it can be observed that mission reliability improvement becomes more significant, namely, three orders versus two orders of magnitude with respect to the optimal mission reliability gains. Note also that the optimal preventive maintenance frequency for the Cruise Phase is now increased to 100, corresponding to a duty period of 6.2 weeks (versus 31.2 weeks). Nonetheless, the optimal preventive maintenance frequency for the Kuiper-Disk Exploration Phase remains 1, which again implies that it will not be beneficial to resume duty-switching after entering the final mission phase (although the reliability gain decreases in a less sensitive manner as n_2 increases, compared with the results shown in Table 2).

To further validate our finding, we apply the model to DS4/Champollion, another X2000 mission mentioned earlier. This mission is designed to visit and study Comet Temple 1 and return a sample to Earth. DS4/Champollion has a 7-year duration. Due to the sample-return nature of this mission, the most critical mission phase — Sampling Phase which demands a full computation power — will reside in the mid-point of the mission as shown in Figure 7.

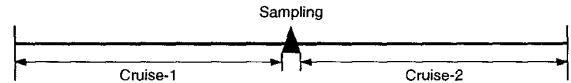


Figure 7: Mission Phases of DS4/Champollion

Tables 4 and 5 (in Appendix B) show the parameter value assignment for the DS4/Champollion study and the corresponding evaluation results, respectively. The results reveal that, preventive maintenance frequencies $n_1 = 20$ and $n_2 = 10$ (corresponding to the duty periods of 9.1 weeks and 18.2 weeks, respectively) will lead to the optimal mission reliability. Thus, unlike Pluto-Kuiper Express, DS4/Champollion favors resuming preventive maintenance in the final mission phase (with a reduced frequency). Explanation for the distinction resides in the differing mission profiles. Specifically, in DS4/Champollion, the residual mission life after the Sampling Phase weighs 50% of the mission life, while in Pluto-Kuiper Express the residual life after the Encountering Phase weighs only about 20% of the mission life. The vulnerability of failure due to component aging in a phase whose duration weighs more significantly with respect to the mission life will have a greater negative impact on mission reliability. As a result, for DS4/Champollion, this vulnerability outweighs the risk of unsuccessful duty-switching and thus necessitates preventive maintenance in the final phase. In other words, whether it is beneficial to conduct preventive maintenance and how often to conduct it de-

pend upon the tradeoffs between the two types of risks described above. Note that the conclusions of our studies are very consistent. That is, the evaluation results from all studies show significant reliability gains from on-board preventive maintenance and suggest to us to exercise preventive maintenance with a reduced frequency or to stop preventive maintenance in the later mission life.

5 Conclusion and Future Work

We have obtained some useful results from the analyses of on-board preventive maintenance for long-life deep-space missions. Our model-based evaluation not only confirms the effectiveness of preventive maintenance but also provides to us further insights regarding the tradeoffs among system and environment attributes and their collective effect on mission reliability gain. From solution method perspective, we have proposed a novel use of Weibull distribution for characterizing and differentiating hardware and software aging and age-reversal processes. The recursive function developed in this paper can be utilized for phased-mission analysis for a variety of space applications, where system attributes have interdependencies between mission phases. For very-long life missions such as Pluto-Kuiper Express, further mission reliability gain may be accomplished through gradual maintenance frequency reduction. For example, the 12-year long Cruise Phase can be divided into a number of segments; maintenance frequency can be adjusted when the mission enters into a subsequent segment. To validate the hypothesis, we plan to conduct analytic and simulation studies. We are also motivated to investigate into the schemes that will further utilize the X2000 architecture's scalability such that the individual strings will be allowed to have various modes of rejuvenation, for example, to operate in different reduced power levels and to accommodate degradable computation quality. The analytic model developed in this paper can be adapted and extended for analyzing those more sophisticated on-board preventive maintenance strategies.

While we are continuing our study for on-board preventive maintenance, we have been investigating into maintenance issues in a broader scope. Similar to the conventional notion of system maintenance, on-board maintenance collectively refers to preservation or improvement, during its operational life, of a system's ability to deliver a service complying with mission requirements. Related issues include evolvability, which permits a spaceborne system, during its mission's long life span, to keep pace with the latest technologies for better performance, fault tolerance and functionality, instead of being constrained by those available prior to mission launch. While evolvability itself can be viewed as on-board perfective maintenance, it necessitates corrective maintenance for detecting and tolerating potential inconsistencies between the old and new system configurations or software versions. Accordingly, how to adapt fault tolerance, dependability and performance engineering techniques to on-board maintenance is a subject of our future research.

References

- [1] L. Alkalai, "NASA Center for Integrated Space Microsystems," in *Proceedings of Advanced Deep Space System Development Program Workshop on Advanced Spacecraft Technologies*, (Pasadena, CA), June 1997.
- [2] L. Alkalai and A. T. Tai, "Long-life deep-space applications," *IEEE Computer*, vol. 31, pp. 37–38, Apr. 1998.
- [3] A. T. Tai, S. Chau, L. Alkalai, and H. Hecht, "On-board preventive maintenance: Analysis of effectiveness and optimal duty period," in *Proceedings of the 3rd International Workshop on Object-Oriented Real-time Dependable Systems (WORDS'97)*, (Newport Beach, CA), pp. 40–47, Feb. 1997.
- [4] Y. Huang, C. Kintala, N. Kolettis, and N. D. Fulton, "Software rejuvenation: Analysis, module and applications," in *Digest of the 25th Annual International Symposium on Fault-Tolerant Computing*, (Pasadena, CA), pp. 381–390, June 1995.
- [5] S. Garg, A. Puliafito, M. Telek, and K. S. Trivedi, "Analysis of software rejuvenation using Markov regenerative stochastic Petri net," in *Proc. 6th International Symposium on Software Reliability Engineering*, (Toulouse, France), pp. 180–187, Oct. 1995.
- [6] S. Garg, A. Puliafito, M. Telek, and K. S. Trivedi, "Analysis of preventive maintenance in transaction based software systems," *IEEE Trans. Computers*, vol. 47, pp. 96–107, Jan. 1998.
- [7] P. S. Ho and T. Kwok, "Electromigration in metals," *Reports on Progress in Physics*, vol. 52, pp. 301–348, Jan. 1989.
- [8] K.-N. Tu, J. W. Mayer, and L. C. Feldman, *Electronic Thin Film Science for Electrical Engineers and Materials Scientists*. Maxwell Macmillan International, 1992.
- [9] L. Alkalai and M. Underwood, "Micro-electronics systems IPDT technology roadmap," Technical Report D-13276, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, Dec. 1995.
- [10] L. Alkalai, J. Klein, and M. Underwood, "The New Millennium Program microelectronics systems, advanced technology development," in *Proceedings of the 34th Aerospace Science Meeting and Exhibit*, (Reno, Nevada), Jan. 1996.
- [11] S. N. Chau, "X2000 avionics system conceptual design document," JPL Technical Report, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, 1997.
- [12] A. Bondavalli, I. Mura, and M. Nell, "Analytical modeling and evaluation of phased-mission systems for space applications," in *IEEE High-Assurance Systems Engineering Workshop*, (Washington, DC), Aug. 1997.
- [13] A. K. Somani and K. S. Trivedi, "Phased-mission system analysis using Boolean algebraic methods," in *Proceedings of 1994 ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems*, (Nashville, TN), pp. 98–107, May 1994.
- [14] J. F. Meyer, "Performability evaluation of the SIFT computer," *IEEE Trans. Computers*, vol. C-29, pp. 501–509, June 1980.
- [15] D. Kececioglu, *Reliability engineering handbook. Volume I*. Englewood Cliffs, NJ: Prentice-Hall PTR, 1991.
- [16] S. M. Ross, *Stochastic Processes*. New York: John Wiley, 2nd ed., 1996.

A Expressions

The expressions for $P[B_{k+1} | A_k]$ and $P[C_{k+1} | A_k]$ (introduced in Section 3.3.1) are as follows.

$$P[B_{k+1} | A_k] = \frac{1}{\prod_{i=1}^k (1 - G[i])} \int_{T_1[k+1]}^{T_2[k+1]} f_{k+1}(x) V_1(k, x) V_2(k, x) V_3(k, x) dx \quad (10)$$

where

$$\begin{aligned} V_1(k, x) &= 1 - \frac{1}{\prod_{i=1}^k (1 - G[i])} \int_{\lfloor \frac{k+1}{2} \rfloor \phi}^{\theta-x} f_{k+1}(y) dy \\ V_2(k, x) &= 1 - \int_0^{x-T_1[k+1]} \hat{f}(t) dt \\ V_3(k, x) &= 1 - \int_0^{\theta-(x+\lfloor \frac{k+1}{2} \rfloor \phi)} \hat{f}(t) dt \end{aligned}$$

And

$$P[C_{k+1} | A_k] = \int_0^\phi \hat{f}(u) W_1(k, u) W_2(k, u) W_3(k, u) du \quad (11)$$

where

$$\begin{aligned} W_1(k, u) &= 1 - \int_0^{\theta-(k\phi+u)} \hat{f}(v) dv \\ W_2(k, u) &= 1 - \frac{1}{\prod_{i=1}^k (1 - G[i])} \int_{T_1[k+1]}^{T_1[k+1]+u} f_{k+1}(x) dx \\ W_3(k, u) &= 1 - \frac{1}{\prod_{i=1}^k (1 - G[i])} \int_{\lfloor \frac{k+1}{2} \rfloor \phi}^{\theta-(T_1[k+1]+u)} f_{k+1}(y) dy \end{aligned}$$

The following are the expressions for γ_i , $T_1[i]$ and $T_2[i]$ for the phased mission analysis (described in Section 3.3.2):

$$\gamma_i = \begin{cases} \lfloor \frac{i-1}{2} \rfloor \delta_1 & i \leq n_1 \\ \lfloor \frac{i-2}{2} \rfloor \delta_1 & i \in \{n_1 + 1, n_1 + 2\} \\ \lfloor \frac{n_1}{2} \rfloor \delta_1 + \lfloor \frac{(i-(n_1+2))-1}{2} \rfloor \delta_2 & n_1 \in \{2l \mid l = 1, 2, \dots\}, \\ & i \in \{n_1 + (2l + 1) \mid l = 1, 2, \dots\} \\ \lfloor \frac{n_1-1}{2} \rfloor \delta_1 + \lfloor \frac{i-(n_1+2)}{2} \rfloor \delta_2 & \text{otherwise} \end{cases} \quad (12)$$

$$T_1[i] = \begin{cases} \lfloor \frac{i-1}{2} \rfloor \phi_1 & i \leq n_1 + 2 \\ (\lfloor \frac{n_1}{2} \rfloor + 1) \phi_1 + \Phi + \lfloor \frac{(i-(n_1+2))-1}{2} \rfloor \phi_2 & n_1 \in \{2l + 1 \mid l = 0, 1, 2, \dots\}, \\ & i \in \{n_1 + 2(l + 2) \mid l = 0, 1, 2, \dots\} \\ \lfloor \frac{n_1}{2} \rfloor \phi_1 + \Phi + \lfloor \frac{(i-(n_1+2))-1}{2} \rfloor \phi_2 & \text{otherwise} \end{cases} \quad (13)$$

$$T_2[i] = \begin{cases} (\lfloor \frac{i-1}{2} \rfloor + 1) \phi_1 & i \leq n_1 \\ \lfloor \frac{i-1}{2} \rfloor \phi_1 + \Phi & i \in \{n_1 + 1, n_1 + 2\} \\ (\lfloor \frac{n_1}{2} \rfloor + 1) \phi_1 + \Phi + (\lfloor \frac{(i-(n_1+2))-1}{2} \rfloor + 1) \phi_2 & n_1 \in \{2l + 1 \mid l = 0, 1, 2, \dots\}, \\ & i \in \{n_1 + 2(l + 2) \mid l = 0, 1, 2, \dots\} \\ \lfloor \frac{n_1}{2} \rfloor \phi_1 + \Phi + (\lfloor \frac{(i-(n_1+2))-1}{2} \rfloor + 1) \phi_2 & \text{otherwise} \end{cases} \quad (14)$$

B Evaluation Results

The following tables supply the parameter values and numerical evaluation results that are referenced and discussed in Section 4.

Table 1: Parameter Value Assignment

θ_1	θ_2	Φ	β	λ	α	μ	ρ	c
624	156	17.3	5.5	0.0005	5.0	0.001	0.50	0.9999999

Table 2: Effect of Maintenance Frequencies on $R(\theta)$, $R_0(\theta) = 0.9995874562$

n_1	n_2				
	1	10	50	100	1000
1	0.9995885863	0.9996769935	0.9996800733	0.9996763954	0.9995955107
5	0.9999888363	0.9999879463	0.9999839475	0.9999789486	0.9998889706
20	0.9999969549	0.9999960546	0.9999920547	0.9999870548	0.9998970611
100	0.999989273	0.9999883728	0.9999843729	0.9999793731	0.9998893799
1000	0.9998993555	0.9998984554	0.9998944559	0.9998894565	0.9997994713

Table 3: Evaluation with a Higher Switching Coverage, $R_0(\theta) = 0.9995874839$

n_1	n_2				
	1	10	50	100	1000
1	0.9995886853	0.9996779012	0.9996845743	0.9996853881	0.9996853485
5	0.9999893313	0.9999893321	0.9999892926	0.9999892426	0.9999883429
20	0.9999989349	0.9999989256	0.9999988856	0.9999988356	0.9999979356
100	0.999999173	0.9999991637	0.9999991238	0.9999990738	0.9999981738
1000	0.9999983504	0.9999983412	0.9999983012	0.9999982512	0.9999973512

Table 4: Parameter Value Assignment for the DS4/Champollion Study

θ_1	θ_2	Φ	β	λ	α	μ	ρ	c
182	182	2	5.5	0.0005	5.0	0.0025	0.50	0.99999999

Table 5: Evaluation Results of the DS4/Champollion Study, $R_0(\theta) = 0.9984515096$

n_1	n_2				
	1	10	50	100	1000
1	0.9981747238	0.9990392929	0.9990390774	0.9990385889	0.9990297644
2	0.9997740022	0.999775253	0.9997748598	0.9997743605	0.9997653715
20	0.9999984255	0.9999996804	0.9999992867	0.9999987867	0.9999897867
100	0.999997648	0.999998903	0.9999985093	0.9999980093	0.9999890093
1000	0.9999886482	0.9999899032	0.9999895095	0.9999890095	0.9999800096