Realization of the Concept of Reasonably Reliable Systems Engineering in the Design of Nano-Satellites

By Seiko Shirasaka1) and Shinichi Nakasuka2)
1)Graduate School of System Design and Management, Keio University, Yokohama, Japan
2)The University of Tokyo, Tokyo, Japan

(Received June 27th, 2011)

High reliability is an essential requirement for avoiding failures in the development of mid-to-large size satellites, which has a major impact on development costs. Conversely, since 2000, several universities have developed and launched low-cost nano-satellites for the purpose of education. Low cost and fast development are key factors in expanding the market for satellites, and balancing cost and reliability becomes a key objective. The theoretical research toward the balance of cost and reliability is being conducted through the government initiative program “New Space Development and Utilization Paradigm for Nano-satellites Introducing Japan-oriented Reasonably Reliable Systems Engineering”.

The objective of this paper is to propose the concept of realizing reasonably reliable systems engineering.

When a system is developed, a standard process is followed1). In particular, the international standard ISO152882) and the US national standards IEEE12203) and ANSI/EIA-6324) are often used for system development. When a satellite is developed, a standard process is also followed such as the ECSS E-105) European standard process for system development. These standard processes define the adopted approach. A process improvement is conducted based on a standard process. 6)

Currently, reliability is based on the assumption that there is no faulty design and reliability depends only on the random failure of parts. However, many real in-orbit failures have been caused by design errors7). Furthermore, in current reliability assessment, recovery is considered as being only part of availability. However, for the customer to receive service from the satellite system, the metric that shows the probability of receiving service is more important. In this paper, we propose a method to calculate a new metric that shows the probability of service and also shows how this method, when applied to nano-satellite design, increases the service probability with low development cost. System reliability is evaluated based on the reliability metric which is defined as the probability that a device will perform its intended function during a specified period of time under stated conditions. 8) The reliability is calculated based on the overall combined failure rate. In this sense, failure is regarded as a random phenomenon. In the new approach, to calculate the probability of service, we use the four types of failure rates as opposed to the one overall failure rate used in normal reliability calculations. These are the combination of temporal failure or permanent failure and random or systemic failure. As far as possible, we aim to recover functionality, thus the temporally failed component should be able to restart after the recovery operation. We applied this method to nano-satellite design. We clearly define the key functions and components which are required to recover failed components. Whereas key components have to be highly reliable and frequently include redundancy, we do not require any redundancy for non-key components. Finally, the probability of service will not decrease significantly when compared with a highly redundant satellite system, even if we have no redundancy for the failure mode with temporal failures.

2. Background

Currently, the scope for applying satellites is very limited. Most satellites are for government missions, especially in Japan. Communication and broadcasting, and remote sensing are commercialized areas. Because of the limited number of satellite developments, it is a difficult field to industrialize. Japanese government satellites are becoming progressively larger. For example, ALOS is about 4 tons and SELENE is about 3 tons. On the other hand, Surrey Satellite Technology LTD (SSTL) has embarked on a new business model using
small satellites (from 100 kg to 500 kg). SSTL sells small satellites to countries that wish to start space systems development. This business model works well at the moment, but international competition is gathering momentum in this rapidly expanding market. There is little or no market for nano-satellites of about 50 kg. (Fig. 19)

To generate a new market for satellite utilization, low cost and fast development are key factors. The balance of cost and reliability is a key aspect of realizing these markets. Professor Nakasuka started the new program “New Space Development and Utilization Paradigm for Nano-satellites Introducing Japan-oriented Reasonable Reliable Systems Engineering” founded as a government-initiated program. This program consists of four themes:

1. Theoretical research on “Reasonably Reliable” Systems Engineering
   - Change the general idea that “Space is expensive”

2. Innovation of nano-satellite equipment to solve the “size” problems
   - New ideas and concepts using new physics, electronics, dynamics, etc.

3. Nano-satellite architecture based on standardized modularity
   - How to drastically reduce costs and development periods.

4. All Japan nano-satellite consortium establishment to combine the competences of Japanese universities and small business.

The first theme is the key concept of this program. Because current space systems are very large and expensive, the customer requires high reliability. This leads to enormous effort and cost. To reach the required reliability level, a system must have redundancy. The design cost increases because of redundancy, and the cost of the tests increases because test cases increase in accordance with redundancy. In addition, there is a large increase in the associated documentation and human resources required. This means an exceptional increase in the costs for a high level of redundancy. (Fig. 20)

In addition, the metric for the reliability itself is not appropriate for evaluating the reliability of the system. The reliability metric is based on the premise that the system will behave as designed, implying that the design is perfect. However, there is the possibility of several design errors becoming apparent in orbit. This means that the reliability metric does not always show the actual reliability.

In reasonably reliable systems engineering, the adequate reliability level is one that does not require too much cost but reaches an adequate level of actual reliability. (Fig. 21)

3. Concept of Reasonably Reliable Systems Engineering

There are two basic concepts of reasonably reliable systems engineering which are very different from the current idea of system development and reliability stated above. Reasonably reliable systems engineering is a development approach which does NOT omit what needs to be done on the ground when dealing with mission failure risks, but reduces the workload needed to ensure successful system operation. The other approach is to reduce cost without decreasing the probability of mission success, even if the level of reliability decreases, because it does NOT show the true probability of system success.
To realize the first concept, we introduce the integral approach to product assurance throughout the project. This is achieved using a “Process Approach.” To realize the second concept, we introduce a new metric for the probability of success as a function of the types of failure. This is realized by the “Product Approach”.

In the process approach, we introduce the integral approach based on a meta-process. Integral design is a well-known Japanese approach to system design in contrast to modular design, which is regarded as a western style of system design. First we define “Meta-process”. Each process has its objectives. A set of objectives is a “Meta-Process” because the set of objectives relates to a set of activities called a “Process”.

If we have a standard process, we can make a standard meta-process which is the set of objectives of the tasks of the standard process. Fig. 3 shows the standard meta-process corresponding to a standard process.

When we conduct a process, we decide which process we will perform, which we will not, and how we will perform it in accordance with the objectives, system and context. When we decide which process we will perform, we coordinate the decision with other stakeholders such as customers, systems engineers, subsystem engineers and component engineers. As a result of this coordination with the stakeholders, we decide on the process. This is the integral approach for process definition.

In the product approach, we introduce a new metric to evaluate system reliability. The current reliability is calculated based only on permanent random failure. However, we have permanent and temporal failures, and both can be random or system failures. A system failure is caused by a design error. Fig. 4 shows the four kinds of failure.

The table below shows the categorization of failures and the countermeasures to them.

<table>
<thead>
<tr>
<th>Categorization of Failures</th>
<th>Counter measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Failure</td>
<td>Normal Red. O</td>
</tr>
<tr>
<td>Systemic Failure</td>
<td>Func. Red. O</td>
</tr>
<tr>
<td>Temporal Failure</td>
<td>Power Cycle O</td>
</tr>
<tr>
<td>Random Failure</td>
<td>Normal Red. O</td>
</tr>
<tr>
<td>Systemic Failure</td>
<td>Func. Red. X</td>
</tr>
</tbody>
</table>

This means that in so far as we can retain recovery...
functionality (power cycle), the temporally failed component can be restarted after a recovery operation. In the case of software, new software can be uploaded even if it has systemic failures (“bugs”) providing the software upload function is working. Table 1 shows the effectiveness of counter measures for each failure. In the new reliability metric, when dealing with recovery, failed components are handled as normal components. Generally normal redundancy, which means duplication of a component, is used to cover a failure. However, this cannot cover systemic failure because the design of the two components is identical. If possible, we use functional redundancy, which means the same function is implemented by a different design. However, we have to develop two components for the single purpose. This is not cost effective. If we use power-cycle, we can cover temporal failure and random failures of the temporal failure. According to the onboard failure analysis performed by Prof. Saito, only 20% of failures are permanent random failures in real projects. This implies that the current normal counter measure, which is normal redundancy, is not effective for real failures.

The current reliability is calculated from the random failure rate of parts. But the new reliability is calculated from the combination of temporal failure rate, permanent failure rate and recovery rate shown in Fig.5.

\[
\lambda_1 : \text{Eternal failure rate} \quad \lambda_2 : \text{Temporal failure rate} \\
\lambda = (1-a) \lambda_2
\]

\(a\) : Recovery rate

Fig. 5: Reliability model with recovery

4. Application of Reasonably Reliable Systems Engineering

In the process approach, there are two application examples, namely the design phase, and the test phase.

At a design review, usually the reviews are only collected and checked to ensure the design is based on the review document. However, if the design of the component is identical to a previous satellite and the same engineer designed it, is a design review really needed? If only the mechanical design of the component is changed from the previous satellite, do we really need a review of the software design? In the process approach, we consider what the objectives of this design review are, who the designer is, what consideration should be given to his or her experience, whether the design is new and whether the customers care about the documentation and so on.

We must decide and clarify whether a review is necessary, who the reviewers should be, and what we should do based on these considerations.

We applied this method to nano-satellite design. We clearly defined the functions and components which are essential for recovering failed components. Typical key components include communication, data handling and electrical power components. Non-key components are the remainder. The key components must be highly reliable, possibly implying the use of redundancy, but redundancy is necessary for non-key components. Finally if the failure modes are temporal failures, the probability of service will not be decreased as much as in highly redundant satellite systems even when we have no redundancy.

In current “mid-to-large” satellite system development, all functions are verified at each level. At the component level, a component level of verification is completed. This is beneficial for mitigating risk, determining any failures after the shipping of the component and being able to return to the previous phase to correct the failure. At the subsystem level, a subsystem level of verification is also completed. Finally system integration starts. At the system level, functional and several other tests are performed.

There are several environmental tests including vibration, shock, acoustic and thermal vacuum testing. After the environmental tests, all functions are tested to clarify whether or not any failure occurred during the environmental test (Fig.6).

The same functional tests can be conducted several times during integration processes. A function is tested at component level. The same test can be performed at a subsystem level as part of the subsystem level functions. Furthermore, the same function can be tested at a system level.
as part of the system level functions. Even at the system level, the same tests can be performed before and after vibration, shock and acoustic tests. They can be performed during thermal vacuum tests and long duration tests. To avoid the risk of jumping back several steps in the case of failure, this process is reasonable. As a standard process for several types of satellite development, this process is also reasonable because a standard process should cover various types of satellites that might require different forms of testing.

If we focus on a specific project, we can carry out different processes. For example, if we use the same component developed by the same well-known engineer, you might rely on his product based on your experience of his products. In this situation, you might accept eliminating some testing that can be replaced by a test performed at the system level. In a different situation in which the same engineer is ordered to develop a new product, you might ask him to conduct all the required tests at a component level because there is a high risk that the new product may have some malfunctions. This approach is very natural in a Japanese environment. Knowing the people who develop the product, the product itself and the context in which the product is being developed, we can deduce the level of risk. If the risk is high, we can ask for verification at each level, but if the risk is low, we can bypass some verification to reduce cost and time. We may have a standard way of adapting the process in accordance with the context instead of following the standard process. This form of development process is called the "integral product assurance approach" because the product assurance process is adapted among component developer, subsystem developer and system developer. Fig. 7 shows the process that uses the new Japanese way.

In the product approach, we provide one example. As detailed in the previous section, there are four kinds of failure and the effective counter measures are different (Table 1). In addition, the method of proving each failure is very different. According to Prof. Sato’s research[7], most of the failures are temporal failures. This means that power-cycle method is a very effective approach to counter measures of in-orbit failures. Based on this investigation, we can design a satellite. To perform a power-cycle operation, electrical power, communication and command processing are required. This means that these functions should be designed to be failure resilient, so their implementation should have redundancy. If possible, functional redundancy is preferred for implementing these functions.

On the other hand, single string implementation is adequate for implementing other functions because they can be restarted by the power-cycle method, providing it functions correctly. Fig. 8 shows the satellite architectural design based on this idea.

![Fig.7 Example of Integral Process](image)

![Fig.8 System Architecture Design example](image)
operational costs. Even with this reduction in costs, there is NO need to prove mission success because single string parts can recover using the power-cycle method even if they have some failures. This is virtually the same as redundancy design.

5. Conclusions

Reasonably reliable systems engineering consists of the process and product approaches.

In the process approach, we propose a meta-process and an integral quality assurance concept. The meta-process is a set of process objectives. When we develop a system, we follow the meta-process instead of the normal process. When we perform this process, we coordinate the contents of the process based on the context and system itself. This realizes an integral quality assurance.

In the product approach, we introduce a new categorization of failures and propose the effective counter measure to each failure category. Current reliability is based on the assumption that there is no faulty design and it depends only on the random failure of parts. However, many real in-orbit failures are caused by design errors. In addition, for current reliability, the recovery is considered to be only part of availability. However, for the customer to receive service from the satellite system, a metric that shows the probability of receiving service is more important. In the new approach to calculate the probability of service, we use four kinds of failure rates instead of the single overall failure rate in normal reliability calculations. These are a combination of temporal or permanent failures and random or systemic failures. In terms of retaining recovery functionality, the temporally failed component can be restarted after the recovery operation. We applied this method to nano-satellite design. We clearly define those functions and components that are key to recovering failed components. The key components must be highly reliable, possibly involving redundancy, while redundancy is not needed for non-key components. We demonstrate with a satellite architecture design example that employs our proposal for effective counter measure.

Acknowledgements

This research is supported by a grant from the Japan Society for the Promotion of Science (JSPS) through the “Funding Program for World-Leading Innovative R&D on Science and Technology (FIRST Program)”, initiated by the Council for Science and Technology Policy (CSTP).

References