International Journal of
Information
and
Management
Sciences

International Journal of Information and Management Sciences
**29** (2018), 415-424. DOI:10.6186/IJIMS.201812_29(4).0005

# Quantitative Mission Risk Assessment of the Satellite Propulsion Subsystem Using PRA Method

*Xiao-Peng Li*[1], *Fu-Qiu Li*[2] *and Hong-Zhong Huang*[1]

[1]University of Electronic Science and Technology of China and
[2]China Astronautics Standards Institute

**Abstract**

The propulsion subsystem provides thrust for the attitude and orbit changes of the satellite. It is very crucial for the satellite mission success, because the occurrences of the system failures may cause the decline of accurate attitude control, reduction of the satellite life, or even the failure of the mission. Mission risk analysis and assessment of the propulsion subsystem has been a key concern in the satellite reliability. Due to the different success criteria, configurations and the component behaviors in the different mission phases, the propulsion subsystem is a typical phased-mission system (PMS). The traditional method of the propulsion subsystem reliability and risk assessment depends on the static RBD model, and neglects the PMS characteristic, so the results can not satisfy the engineering requirements. This paper proposes a quantitative mission risk assessment method based on the probabilistic risk assessment (PRA) technology and use the software to get the quantitative assessment and the order of the risk importance results.

*Keywords:* Propulsion subsystem, quantitative mission risk assessment, PMS, PRA.

## 1. Introduction

As one of the most important subsystems in the satellites, the propulsion subsystem provides the thrust, which will be used to change or maintain the satellite attitude or orbit. The failures of the propulsion subsystem may cause the satellite to lose attitude or orbit, reduce the satellite life, or even the loss of the satellite mission. So, the mission risk assessment has been a key concern in the satellite reliability work. The propulsion subsystem is one typical phased-mission system (PMS). Zhai et al. [19] proposed an aggregated combination reliability model for non-repairable PMS, and Li et al. [13] shown the reliability assessment process of multi-state PMS. Li et al. [14] gave the reliability analysis of PMS with non-exponential and partially repairable components. Wang er al. [17] and Wang et al. [16] analyzed the probabilistic competing failure in PMS. The PMS is the most important characteristic of the aerospace system. The Probabilistic Risk Assessment (PRA) technology is developed by the NASA and used

in most aerospace programs. Denning and Budnitz [5] gave the impact pf PRA and severe accident research in reducing reactor risk, and Kwag et al. [11] demonstrated the model validation method using Bayesian Network. Zhang et al. [20] gave the integrated modeling approach of PRA method, and Lewandowski [12] proved the implementation of condition-dependent PRA method. Zhou et al. [22] gave an improved Multi-unit nuclear plant seismic PRA approach.The traditional quantitative mission risk assessment method in Engineering is the reliability block diagram (RBD)model. Ahmed et al. [2] gave the formalization of RBD, and Kaczor et al. [10] and Ding et al. [6] used RBD method to analyze the system reliability and safety. This traditional process, where the engineers will build the RBD model of the propulsion subsystem first, and then calculate the system mission reliability through the components reliability data, has the following defects: a) does not consider the multi-state feature of the system mission; b) can not give the order of the risk importance. These problems lead some difficulties to the subsystem designers and product assurance personnel to find the failure causes of the subsystem failures on the orbit in time. In order to solve these problems, this paper proposes a quantitative risk assessment method based the PMS characteristic and PRA method.

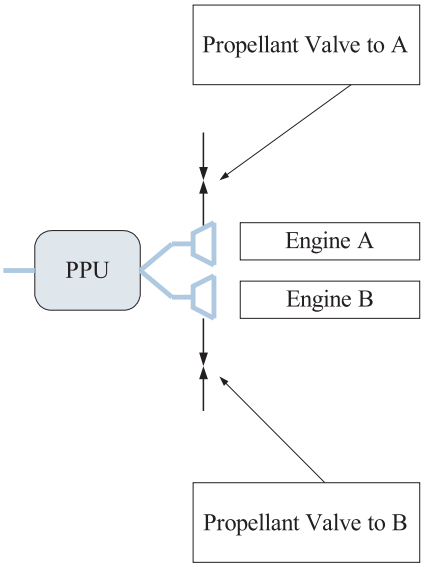


Figure 1: Propulsion subsystem block diagram.

## 2. Propulsion Subsystem

### 2.1. Structure of the system

Mandelli et al. [15] indicated that the propulsion subsystem in this paper consists of a propulsion power unit (PPU), a main engine (Engine A), and an engine (Engine B) in stand by redundancy, and a propellant valve for each engine, as described in Figure 1. The propulsion subsystem has four operational modes: Start-Up, Operation,

Non-Operation and Shut-Down. When the system is operating, the PPU provides power to only one engine, and the other engine will be in a standby mode, which operates until the former engine failed. When engine A fails, the strategy is to shut down the PPU, switch the PPU to engine B, reenergize the PPU, and operate with engine B. Azarkhail and Modarres [3] introduced that the propellant valves will open (close) to supply (isolate) propellant flow to each engine.

### 2.2. Mission phases of the system

Three mission phases will be considered for the propulsion subsystem: the attitude adjustment (AA) phase, the attitude maintenance (AM) phase, and the orbit movement (OM) phase. In the AA phase, the mission success criterion is having only one engine operations of the two engines due to small thrust demanded.

When the system is in the AM phase and the propulsion is not needed, the mission requires the operational engine in the former phase to be shut down. In the last phase, all the two engines will be needed to operate because of the large thrust requirement. Figure 2 shows the phase divisions and the number of engines required for each phase along with the mission time.

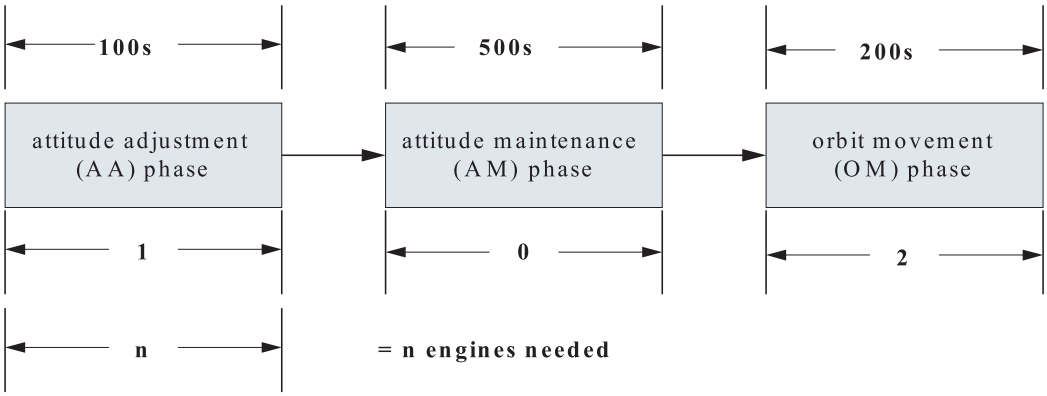


Figure 2: Mission phases of the propulsion subsystem.

### 2.3. Reliability data of the propulsion subsystem components

The system includes the components of the propellant valves, the PPU and engines. Different failures of these components will cause different effects on the system mission. The objective of the analysis for the propulsion subsystem is to evaluate the system risk during the mission phases based on the components reliability data, as shown in Table 1. The failure which occurs at the specific time that an item is called upon demand to function, and the outcome of such a failure is binary, either success or loss. The failure is quantified by probability of occurrence/non-occurrence. The failure occurs over an interval of time, for which the probability of failure over the length of the interval is expressed as a point estimate.

Table 1: Reliability data of the space propulsion subsystem components.

| Components | Failure Mode | Failure Probability /Failure Rate | Effect |
|---|---|---|---|
| Propellant Valve | Fails to Open on demand | $3 \times 10^{-4}$(per demand) | Loss of Engine |
| | Fails to Close on demand | $3 \times 10^{-4}$(per demand) | System Failure |
| | External Leakage | $5 \times 10^{-5}$(per hour) | System Failure |
| PPU | Fails to Start on demand | $1 \times 10^{-4}$(per demand) | System Failure |
| | Fails to Operate | $1 \times 10^{-6}$(per hour) | |
| | Fails to Shut Down | $1 \times 10^{-5}$(per hour) | |
| | Fails to Switch Engine B | $2 \times 10^{-6}$(per demand) | |
| Engine | Fails to Start on demand | $3 \times 10^{-5}$(per demand) | Loss of Engine |
| | Fails to Operate | $2 \times 10^{-5}$(per hour) | |
| | Fails to Shut Down | $3 \times 10^{-6}$(per demand) | |

## 3. Quantitative Risk Assessment Model of the System

The mission procedure of the propulsion subsystem shows that it is a typical PMS, which is defined as a system whose mission is composed of multiple, consecutive and non-overlapping phases. Xing and Dugan [18] analyzed the PMS configuration, success criteria, and component failure behaviors's changes from phase to phase. PRA is a proper method for building the risk model of the propulsion subsystem. PRA is a comprehensive, structured, and logical analysis method aimed at identifying and assessing reliability and risk in complex technological systems.

Gupta and Nouri [9] analyzed this method s purpose of cost-effectively improving safety and performance. PRA can assess the mission reliability of a complex space system with event tree (ET) and fault tree (FT) model.

In this paper, the initial events (IE) of the system components will be analyzed and determined first. Then the system events sequence diagrams (ESD), which used by Zhou et al. [21] and Campean and Yildirim [4] will be built after determining the pivotal events (PE) of each ESD. Then the IE and PE of each ESD will be quantified and integrated through the software tool Quantitative Risk Assessment System (QRAS), which introduced by Groen et al. [8]. As a PRA tool, it provides the capability of modeling the hierarchical structure of the system and dividing the system operation into phases and sub-phases. QRAS allows the aggregation of the end state results in the system and sub-systems. This integrated environment for modeling system PRA, right from system hierarchy to basic event level probability models, differentiates QRAS from other available PRA tools.

### 3.1. Initial events of the system components

Each component of the system has multi failure modes. Some failure modes will lead the system or the satellite mission failure, these failures modes should be considered as

Table 2: IE of each System Component.

| Component | IE | Failure Probability/Rate | Effect |
|---|---|---|---|
| Propellant Valve | External Leakage | $5 \times 10^{-5}$(per hour) | System Failure |
| PPU | Fails to Switch Engine B | $2 \times 10^{-6}$(per demand) | System Failure |
| Engine | Fails to Operate | $2 \times 10^{-5}$(per hour) | Loss of Engine |

IEs and analyzed the sequential results. The IE of each system component is shown in Table 2.

### 3.2. Pivotal events for each IE

(1) When the external leakage occurs, the control system will try to detect the failure, and if the failure is detected, the propellant valve will be closed, and the system mission will degrade, or the failure will lead fires in the propulsion subsystem and the mission will be ended.
(2) When the engine A failed, the PPU will be shut down, and switch to the engine B and reenergized again. At last, the PPU will operate with engine B. When the PPU fails to switch to the Engine B, because of the loss of the thrust, the system mission will fail.
(3) When the engine fails to operate, the control system will close the engine, and the PPU will switch to the redundant engine, which will be started on demand. If the redundant engine fails to start on demand, the system will lose all engines.

### 3.3. Event sequential diagrams for the system

The propulsion subsystem has three IEs, and the PEs of each IE are given above. Define that the system has three mission result states, the mission success state, the mission degradation state and mission failure state respectively. Then the ESDs of the system can be described through Figure 3 to Figure 5.

### 3.4. Model of the quantitative mission risk assessment

The three IEs of the system components will occur in different mission phases. For example, the "external leakage" IE will occur during any mission phase, but the "fails to switch Engine B and fails to operate" IEs will not occur in the AM phase without thrust requirements. The model of the quantitative mission risk assessment will be built in accordance with the following steps:

- Create the project and build the hierarchy;
- Define the mission phases;
- Define operational time intervals (OTI) and IEs applicability;

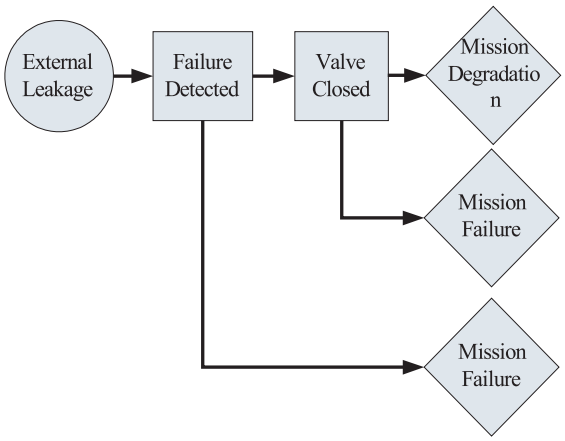


Figure 3: The ESD of the propellant valve IE external leakage.


Figure 4: The ESD of the PPU IE failed to switch engine B.

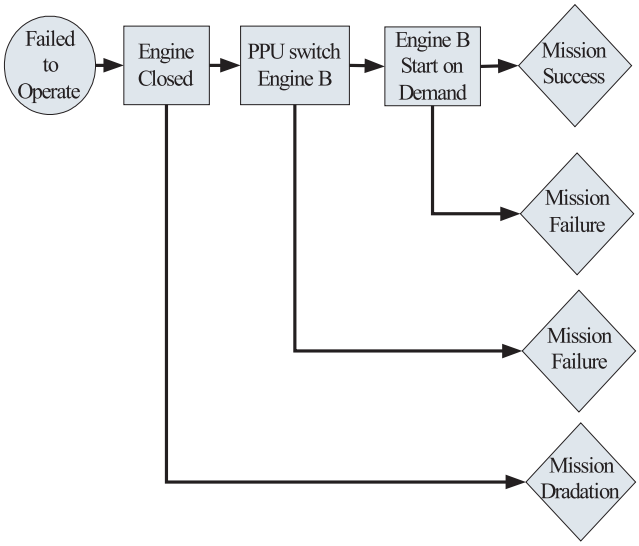


Figure 5: The ESD of the engine IE failed to operate.

- Create ESDs;
- Quantify IEs and PEs;
- Associate ESDs to OTIs.

Above all, the model of the quantitative mission risk assessment will be built through the software tool QRAS and shown in Figure 6.

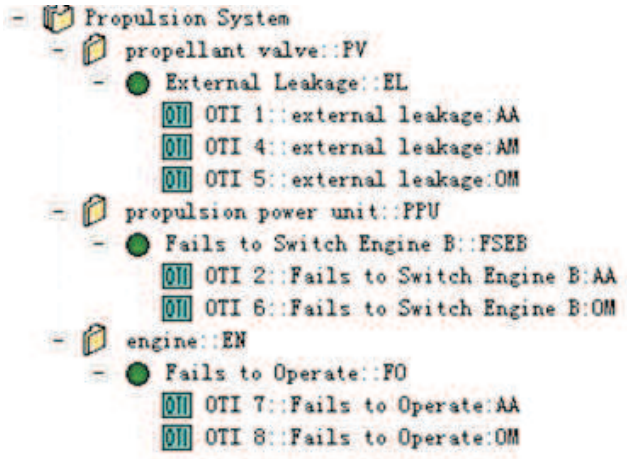


Figure 6: The model of the quantitative mission risk assessment for the propulsion subsystem.

## 4. Quantitative Risk Assessment Results

After building the model of the quantitative mission risk assessment for the propulsion subsystem, then the assessment and analysis can be carried out through the software QRAS.

### 4.1. System level analysis

Select the propulsion subsystem at the highest level on the Master Logic panel, and run the analysis at this level to view the results, and the occurrence probabilities for end states of the propulsion subsystem are shown in Table 3.

The propulsion subsystem risk assessment results can be gotten from the above end states risk assessment results. The results show that the MD end states has a 0.04108mean probability of occurring due to the logic of the ESDs and OTIs associated with the system, and MS end states has a 24.1% mean probability of occurring due to the logic of the ESDs and OTIs associated with the system, respectively.

Because the IEs of the propulsion subsystem are some fatal failures, so the system MF end state probability is much higher than the others, and this result meets the engineering practice.

### 4.2. Components level Analysis

Select the propellant valve, the PPU and the engine components respectively on the Master Logic panel respectively and run the analysis at component level to view the results, and the assessment results of the propulsion subsystem end states caused by the system components are shown in Table 4.

Table 3: The occurrence probabilities for end states.

| End State | Confidence Level | Occurrence Probabilities |
|---|---|---|
| MS | Mean | 0.241 |
| | 95% | 0.06432 |
| | 5% | 0.4323 |
| MD | Mean | 0.0004108 |
| | 95% | 0.001006 |
| | 5% | 0.0009074 |
| MF | Mean | 0.6064 |
| | 95% | 0.2861 |
| | 5% | 0.8084 |

Table 4: The assessment results of the propulsion subsystem end states caused by the system components.

| Component | End State | Mean Occurrence Probabilities |
|---|---|---|
| Valve | MD | 0.0001028 |
| | MF | 0.6052 |
| PPU | MF | 0.002393 |
| Engine | MS | 0.241 |
| | MF | 0.0006171 |
| | MD | 0.0003079 |

The propellant valve is the main component which causes the propulsion subsystem to fail based on the results above, and some design improvement actions can be suggested to the propellant valve to reduce the risk.

## 5. Conclusions and Future Works

This paper uses the PRA technology to quantitatively assess the propulsion subsystem mission risk. Although PRA is widely used to assess the complex system mission risk, but it is difficult to model and analyze some special characteristics of the propulsion subsystem, such as cold spare (CSP) engine in the propulsion subsystem. It is necessary to use some new methods to solve this problem. There are two frequently-used methods

in Engineering, dynamic fault tree (DFT) method and Bayesian networks (BNs) method respectively.

The traditional FT method normally useful for the static system reliability, can not analyze the dynamic characteristics of the system. In order to solve this problem, Abdo and Flaus [1] introduced the DFT method by adding sequential notion through introducing the dynamic gates to the traditional FT method. Therefore, the system failures can then depend on the orders of component failures as well as combinations. DurgaRao and Gopika [7] shown the modeling power of DFT, which gained the attention of many reliability engineers working on safety critical systems.

BNs are increasingly used for various areas of the complex system reliability models, risk management, and safety analysis based on probabilistic and uncertain knowledge. BNs takes advantage of the "d-separation" criterion and the chain rule to perform quantitative analysis. Zitrou et al. [23] demonstrated that based on d-separation criteria, all root nodes are conditionally independent and the other nodes are conditionally dependent on only their direct parents.

In the future works, the DFT and BNs methods will be used to model and quantify the pivotal events, which describe the redundancy features, operation sequence dependencies, and relevant failure properties of some components. At last, analyze and aggregate the components and scenarios risk in all the phases through the uncertainty analysis and Monte Carlo simulation to give the complex system mission risk analysis result.

## References

[1] Abdo, H. and Flaus, J. (2016). *Monte Carlo simulation to solve fuzzy dynamic fault tree*, Ifac Papers online, Vol.49, No. 12, 1886-1891.

[2] Ahmed, W., Hasan, O. and Tahar, S. (2016). *Formalization of reliability block diagrams in higher-order logic*, Journal of Applied Logic, Vol.18, 19-41.

[3] Azarkhail, M. and Modarres, M. (2006). An Intelligent Agent-Oriented Approach to Risk Analysis of Complex Dynamic System with Applications in Planetary Mission, in Proc. of the 8th Int. Conf. On Probabilistic Safety Assessment and Management, PSAM-0202.

[4] Campean, F. And Yildirim, U. (2017). *Enhanced sequence diagram for function modelling of complex systems*, Procedia Cirp, Vol.60, 273-278.

[5] Denning, R. and Budnitz, R. (2017). *Impact of probabilistic risk assessment and severe accident research in reducing reactor risk*, Progress in Nuclear Energy, Vol.102, 90-102.

[6] Ding, L., Wang, H. and Jiang, J. (2017). *SIL verification for srs with diverse redundancy based on system degradation using reliability block diagram*, Reliability Engineering & System Safety, Vol.165, 170-187.

[7] DurgaRao, K. and Gopika, V. (2009). *Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment*, Reliability Engineering and System Safety, Vol.94, 872-883.

[8] Groen, F., Smidts, C. and Mosleh, A. (2006). *QRAS - The quantitative risk assessment system*, Reliability Engineering & System Safety, Vol.91, No. 3, 292-304.

[9] Gupta, A. and Nouri, K. (2006). QRAS Approach to Phased Mission Analysis, in Proc. of the 8th Int. Conf. On Probabilistic Safety Assessment and Management, PSAM-0444.

[10] Kaczor, G., Młynarski, S. and Szkoda, M. (2016). *Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams*, Journal of Loss Prevention in the Process Industries, Vol.41, 31-39.

[11] Kwag, S., Gupta, A., and Dinh, N. (2018). *Probabilistic risk assessment based model validation method using bayesian network*, Reliability Engineering & System Safety, Vol.169, 380-393.

[12] Lewandowski, R., Denning, R. and Aldemir, T. (2016). *Implementation of condition-dependent probabilistic risk assessment using surveillance data on passive components*, Annals of Nuclear Energy, Vol.87, 696-706.

[13] Li, X., Huang, H. and Li, Y. (2018). *Reliability assessment of multi-state phased mission system with non-repairable multi-state components*, Applied Mathematical Modelling, Vol.61, 181-199.

[14] Li, X., Huang, H. and Li, Y. (2018). *Reliability analysis of phased mission system with non-exponential and partially repairable components*, Reliability Engineering & System Safety, Vol.175, 119-127.

[15] Mandelli, D., Aldemir, T. and Zio, E. (2006). An Event Tree/Fault Tree/Embedded Markov Model Approach for the PSAM-8 Benchmark Problem Concerning A Phased Mission Space Propulsion subsystem, in Proc. of the 8th Int. Conf. On Probabilistic Safety Assessment and Management, PSAM-0318.

[16] Wang, C., Xing, L. and Peng, R. (2017). *Competing failure analysis in phased-mission systems with multiple functional dependence groups*, Reliability Engineering & System Safety, Vol.164, 24-33.

[17] Wang, Y., Xing, L.and Levitin, G. (2018). *Probabilistic competing failure analysis in phased-mission systems*, Reliability Engineering & System Safety, Vol.176, 37-51.

[18] Xing, L. and Dugan, J. B. (2002). *BDD-based reliability analysis of phased-mission systems with multimode failures*, IEEE Trans. Reliability, Vol.51, No. 2, 199-211.

[19] Zhai, Q., Xing, L. and Peng, R. (2018). *Aggregated combinatorial reliability model for non-repairable parallel phased-mission systems*, Reliability Engineering & System Safety, Vol.176, 242-250.

[20] Zhang, S., Tong, J. and Zhao, J. (2016). *An integrated modeling approach for event sequence development in multi-unit probabilistic risk assessment*, Reliability Engineering & System Safety, Vol.155, 147-159.

[21] Zhou, J., Reniers, G. and Khakzad, N. (2016). *Application of event sequence diagram to evaluate emergency response actions during fire-induced domino effects*, Reliability Engineering & System Safety, Vol.150, 202-209.

[22] Zhou, T., Modarres, M. and Droguett, E. (2018). *An improved multi-unit nuclear plant seismic probabilistic risk assessment approach*, Reliability Engineering & System Safety, Vol.171, 34-47.

[23] Zitrou, A., Bedford, T. and Walls, L. (2010). *Bayes geometric scaling model for common cause failure rates*, Reliability Engineering and System Safety, Vol.95, 70-76.

School of Mechanical and Electrical Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China.

E-mail: lixiaopeng200501@163.com

Major area(s): System reliability and safety.

Reliability Engineering Department, China Astronautics Standards Institute, Beijing, 100071, China.

E-mail: lifuqiu2004@126.com

Major area(s): System reliability and safety.

School of Mechanical and Electrical Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China.

E-mail: hzhuang@uestc.edu.cn

Major area(s): Reliability design and optimization design, state monitoring, fault diagnosis and life prediction, digital Design and Intelligent Manufacturing.

(Received September 2018; accepted November 2018)