Reliability design of aerospace secondary power supply based on fault tree analysis

Ting Gao¹,², Mi Liu², Hong-Yi Qu¹, Hong-Juan Ji¹ and Jiang Jing¹

¹ Beijing Institute of Space Long March Vehicle, Beijing, China
² Beijing Spacecrafts, Beijing, China

E-mail: 418206250@qq.com

Abstract. As the satellite power supply and distribution functions and complexity are gradually strengthened, the reliability requirements of the aerospace secondary power supply are getting higher and higher. Based on the basic composition and working principle of aerospace secondary power supply, this paper analyzes the reliability of the fault tree analysis method (FTA), combs the weak link of the product, and proposes design improvement measures for the weak link.

1. Introduction

The aerospace secondary power supply is the basic unit of the spacecraft power supply and distribution system, and its reliability is directly related to the reliability and mission success of the entire system. At present, the secondary power supply of aerospace mainly includes three busbar series of 28V, 42V and 100V, and the power levels are mainly distributed in the range of 5W to 200W [1]. With the increasing integration and complexity of aerospace electronic products, the demand for aerospace secondary power products is becoming smaller, more efficient, high power density and diversified. The stringent requirements imposed by the new type of load on the secondary power supply pose greater challenges to the reliability design [2-4] of the already complex secondary power supply. At present, FMEA method is often used to identify product failure modes in reliability design process. FTA based on unacceptable failure mode of products is not carried out, so there is a risk of missing identification of design weak links. In this paper, the FTA method is used to identify the weak points of design, formulate improvement measures, and improve the reliability of product design.

2. Aerospace secondary power supply composition and working principle

The aerospace secondary power supply is usually a modular switching power supply, and the switching power supply is a high frequency switching energy conversion electronic circuit. The switching power supply is the abbreviation of the switching power supply. The power semiconductor device is driven as a switching element by pulse width modulation (PWM), and the output voltage is adjusted by controlling the duty ratio of the switching element by a periodic on/off switch [5]. The aerospace secondary power supply mainly includes an input circuit, a power conversion circuit, a rectification and filtering output circuit, a control circuit and an auxiliary power supply, as shown in Figure 1.

The input circuit includes a fuse protection circuit, a surge suppression circuit, and an EMI filter circuit. The fuse protection circuit is a first-level protection of the secondary power supply of the
aerospace. When the input stage is short-circuited, the power supply is quickly disconnected from the primary bus; the surge suppression circuit[6] limits the surge current of the power supply to prevent the surge current from being too large. The level distribution link affects; the EMI filter circuit ensures that the power supply product meets the spacecraft electromagnetic compatibility requirements. The power conversion circuit comprises a main power transformer and a power switch tube, which is a secondary power core module, and realizes magnetic isolation power conversion and transmission of input and output. The rectified filter output circuit rectifies the output voltage to pulsating DC and smoothes to a low ripple DC voltage. The control circuit integrates the voltage and current detection signals, and outputs the modulated control pulses to achieve the purpose of adjusting the output voltage. The auxiliary power supply provides the voltage required by the control circuit during the secondary power supply starting process. After the secondary power supply output voltage is established, the auxiliary power supply can be taken out of the loaded state by the feedback power supply.

![Figure 1](image1.png)

Figure 1. Diagram of the aerospace secondary power function

3. Aerospace secondary power reliability

3.1. Aerospace secondary power supply reliability model

The reliability mathematical model is based on the reliability block diagram, and uses mathematical expressions to express the mathematical relationship between the system reliability and the components. According to Figure 1, combined with the basic working principle of the aerospace secondary power supply, the reliability block diagram is shown in Figure 2. As can be seen from the block diagram, the functional modules of the aerospace secondary power supply are in series.

![Figure 2](image2.png)

Figure 2. Aerospace secondary power supply reliability block diagram

For a series system, any unit failure in the system will cause the system to fail, so the life of the series system depends on the unit with the shortest life of all the components. Suppose that the series system is composed of n units, the life of the ith unit is ti, then the reliability of the series system[7] is:

$$ R_S(t) = P(T_S > t) = P(t_1 > t, t_2 > t, \ldots, t_n > t) = \prod_{i=1}^{n} R_i(t) = \prod_{i=1}^{n} e^{-\lambda_i t} $$

The reliability of the aerospace secondary power supply can be expressed as:
3.2. Aerospace secondary power supply reliability prediction

Reliability is expected to be based on the product reliability model, based on the fault data and related data obtained during the development process and use of similar or similar products, to predict the level of reliability that the product and its units can achieve in actual use.

Data source for aerospace secondary power supply reliability prediction: Components are estimated according to GJB/Z299C[8]. The methods and steps for predicting the reliability of aerospace secondary power supply are as follows:

1. Using the component stress method, first analyze the environmental stress and electrical stress of each component in the product, and calculate the failure rate of each component;
2. The failure rate of each component in the function module is added to obtain the failure rate of the functional module;
3. According to the reliability block diagram (model) of the secondary power supply, the task reliability of the expected product is combined with each task stage.

When aerospace secondary power products are expected to be reliable, they must first complete the derating design and thermal design of the product. Reliability is estimated according to the highest electrical stress and thermal stress of the actual working conditions of the product. Table 1 shows the expected results of a typical aerospace secondary power supply with an input of 100V, an output of 50W28V, and an in-orbit design life of 15 years.

Table 1. 50W28V aerospace secondary power supply reliability prediction results (70 °C).

| Serial number | Module unit name                                | Reliability       |
|---------------|-----------------------------------------------|-------------------|
| 1             | Fuse protection and surge suppression circuit  | 0.99837315        |
| 2             | Input EMI filter circuit                       | 0.99807526        |
| 3             | Auxiliary power circuit                        | 0.99621010        |
| 4             | Control circuit                                | 0.99032243        |
| 5             | Power conversion circuit                        | 0.99597773        |
| 6             | Output rectifier filter circuit                 | 0.99874067        |
| total         |                                               | 0.97788121        |

Reliability is expected to evaluate the quantitative indicators of the overall reliability design of secondary power products. It can identify high-loss function modules, but it cannot give the severity of product failure caused by specific component failures. The tree analysis method focuses on identifying the weak points in the design of high failure devices.

4. Aerospace secondary power fault tree analysis

The fault tree analysis method[9] is a graphical deduction method used to indicate that failures of those components that make up a product result in a given failure mode for the product. Fault tree analysis uses a certain failure mode that may occur in the system as the top event, and uses the specified logical symbols to identify all the direct factors and causes that cause the top event. These factors and causes are intermediate events in the transition state. And gradually analyze it until the most basic cause of the accident, that is, the bottom event of the fault tree.

The main function of the aerospace secondary power supply is to convert the satellite primary bus voltage into a smooth secondary voltage output. In the secondary power supply design process, priority is given to product failures that cannot affect a busbar. The front end of the product is equipped with a fuse protection circuit, so there is no fault mode in the secondary power supply that
causes a busbar short circuit. Generally, the main performance of the secondary power supply failure is that the product has no output (Note: the output voltage is lower than the task requirement value is regarded as no output), so the fault tree is established with the "Secondary power supply no output" as the top event T.

**Figure 3.** Aerospace secondary power "no output" fault tree.

**Table 2.** Aerospace secondary power failure tree event number and significance.

| Numbering | Meaning                                      |
|-----------|----------------------------------------------|
| T         | No output of secondary power supply         |
| B         | Surge suppression open circuit              |
| C         | Input filter open                            |
| D         | No output of auxiliary power supply         |
| E         | Control circuit abnormality                 |
| F         | Power conversion circuit failure            |
| G         | Output filtering failure                    |
| E1        | Control pulse width anomaly                 |
| E3        | Drive no output                             |
| X1        | Fuse open circuit                           |
| X2        | Surge suppression tube open circuit         |
| X3        | Surge suppression tube base slow capacitor short circuit |
| X4        | Input common mode inductor open             |
| X5        | Input differential mode inductor open       |
| X6        | Auxiliary power transformer failure         |
| X7        | Oscillating triode failure                  |
| X8        | Filter capacitor short circuit              |
| X9        | Feedback resistor open circuit              |
| X10       | Control chip peripheral device failure      |
| X11       | Chip failure                                |
| X12       | Overvoltage detection circuit is abnormal   |
| X13       | Drive transformer failure                   |
| X14       | Drive DC blocking capacitor failure         |
As can be seen from the fault tree of Figure 3, the occurrence of any bottom event will result in a system top event. Therefore, all the bottom events are the minimum cut sets of the system, which is a weak link, and the reliability design guarantee is required for each link.

5. Aerospace secondary power supply reliability design
The reliability design of aerospace secondary power supply includes two aspects, one is to improve the reliability of the secondary power supply itself, and the other is to improve the reliability of the secondary power system through the system design during use.

5.1. Aerospace secondary power supply self-reliability design
The design of aerospace secondary power supply is a system engineering, not only to consider the implementation of indicators, but also to consider the reliability of product space applications. Through the fault tree analysis, the weak link causing the secondary power failure is the key device failure of each functional module. In addition to selecting high-quality aerospace-class components, the measures to improve reliability are shown in Table 3.

Table 3. Reliability design measures for the weak link of aerospace secondary power supply.

| Weakness                  | Reliability design measures                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------|
| Fuse                      | Both the bus fuse capacity and the I²t derating are taken into consideration, and the filter matching is used in parallel to improve the uniformity. |
| Resistance, capacitance, diode | Derating design, thermal design; busbar filter and other key parts of the capacitor for series redundancy, strengthen the mechanical design of ceramic capacitors and glass-encapsulated diodes. |
| Power MOS transistor, triode, integrated circuit | Derating design, thermal design, antistatic design, anti-radiation design. The design margin of β value of triode should be increased to cope with its attenuation in space environment. |
| Magnetic device           | Increase the design margin of β value of power transformer under extreme conditions.            |

In addition to the above reliability design measures, for the weak links of reliability analysis, it is necessary to continuously improve the safety and reliability of the aerospace secondary power supply through measures such as safety design, electromagnetic compatibility design, and three-proof design.

5.2. Reliability design of aerospace secondary power system
It can be seen from the FTA of the secondary power supply of the aerospace that there are many weak links that cause the "no output" fault of the secondary power supply, and a large number of device-level redundant backups cannot be performed inside the power supply. Therefore, in addition to strengthening the weak link of the secondary power supply itself. The reliability design also needs to improve the reliability of the secondary power system task through power backup. The typical backup
application connection mode is shown in Figure 4. The main features of each backup mode are shown in Table 4.

![Backup Modes Diagram](image_url)

(a) Hot backup  
(b) Cold backup  
(c) Cross-cold backup

**Figure 4.** Aerospace secondary power supply typical backup connection.

**Table 4.** Comparison of typical backup methods for aerospace secondary power supply.

| Backup method         | Reliability design measures                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------|
| **Hot backup**        | No need to switch the circuit, the load can be uninterrupted power supply, the main and standby switching voltage difference is small, there is a possibility of common cause failure. Two sets of switch circuit are required, and the main and standby circuits are relatively independent, and there is no common cause failure. |
| **Cold backup**       | Six sets of switch circuit are required, the remote control circuit is complicated, the power supply and load cross utilization is high, and there is no common cause failure. |
| **Cross cold backup** |                                                                                                                                 |

The use of aerospace secondary power backup can greatly improve the reliability of the power supply of the secondary power system. For satellite platform power equipment, power supply requirements can not be interrupted equipment, hot backup redundancy can be used, but need to avoid the common cause failure, you can avoid the common cause failure through the load front-end series fuse, current limiting resistor. For load-type power equipment, the active-standby switchover can be implemented by the switch-on command. Cold backup redundancy can be used to save energy while avoiding common cause failure.

By improving the design of the weak link identified by FTA method, the reliability of the product analyzed in this paper is improved from 0.97788121 to 0.980152736. The reliability of the system can reach more than 0.999 through product backup. The design reliability of the product is effectively improved.

**6. CONCLUSIONS**
This paper briefly describes the reliability analysis method of aerospace secondary power supply, and combs the weak link of the secondary power supply “no output” fault mode through FTA, and then gives the design of improving the secondary power supply and mission reliability of the aerospace method. The FTA secondary power supply FTA helps identify weak links at the beginning of product design and provides a basis for product design improvement and troubleshooting.

The reliability of aerospace secondary power is not only related to electrical design, but also related to structure, process, process control, and application conditions. In practical engineering applications, the index system and the application environment should be comprehensively considered, and the products should be tested and verified through mechanics, thermal, EMC and other tests to continuously improve the reliability of the aerospace secondary power products.

References
[1] Chengan W, Lei Y and Jianqiang L 2009 Spacecraft Engineering 18: 15-7
[2] Beibei W, Haibo L, Tingzhong L and Li L 2015 Spacecraft Environment Engineering 32: 73-5
[3] Xiaopeng W, Ping Y and Dongjing L 2011 Information and Electronic Engineering 9: 441
[4] Shibin W, Xihe Y and Jian S 2014 Chinese Journal of Power Sources 38: 317-9
[5] Zhansong Z, Xuansan C 2004 Principle and Design of Switching Power Supply (Beijing: Publishing House of Electronics Industry) 24
[6] Peide D, Xiang L and Yizhi Y 2018 Microelectronics 48: 217-20
[7] Baozhong L 2013 Essentials of Certified Reliability Engineering (Beijing: China Machine Press) 22
[8] GJB/Z 299C 2006 Reliability prediction handbook for electronic equipment
[9] Marvin Rausand 2017 System Reliability Theory: Models, Statistical Methods and Applications (Beijing: National Defense Industry Press) 52-6