한국소음진동공학회 창립 20주년 기념 2010년 춘계학술대회논문집, pp.554~555

인공위성 시스템의 내고장 다중화 설계

Fault-Tolerant Redundancy Management Design of Satellite System

천이진† · 채태병* · 오승엽** · 김은규***

Yee-Jin Cheon, Tae-Byeong Chae, Seung-Hyeub Oh and Eun-Kyou Kim

1. Introduction

A satellite system has redundancy (multiple redundancy) architecture and its associated on-board management scheme to make system safe when anomalies or faults occur. Generally, fault-tolerant redundancy management design is a concept to perform on-board surveillance and to ensure the system safety by on-board functions implemented in either hardware or software (or both).

For a fault-tolerant redundancy management design, the followings have to be taken into consideration:

- System's operational characteristics
- Design complexity .vs. operational flexibility
- Prevention and Isolation of fault propagations
- Interference between subsystems

The following terms are defined for fault-tolerant redundancy management.

- Side A/Side B: Physical location of units
- Primary/Redundant:
  Operational units for system operations
- Hot/Cold: Powered-on/off units
- Active/De-active: Units that are functioning

The term " Active" represents operational status and implicitly includes powered-on status. The terms " Hot" and " Standby" represent powered-on status and non-operational status, respectively. Figure 1 shows an example of units (subsystems) in a system with redundancies.

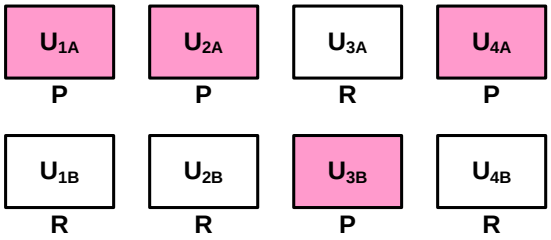

Figure 1 Units (Subsystems) for Redundancy Management

2. Fault-Tolerant Redundancy Management Designs and Operations

2.1 K of N (N>K) Redundancy

In this architecture, system requires K operational units, but N units exist for the redundancy. (N-K) units remain cold. When one or more units of K units, unit (s) of (N-K) will be replaced with failed unit (s). The replacement will be done by either ground-command or on-board function, called on-board fault management (OFM).

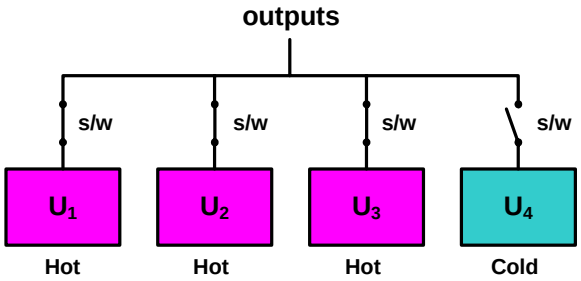

Figure 2 K of N (N>K) Redundancy Architecture

2.2 K of N Active Redundancy

K of N active redundancy architecture requires K operational units, but N units exist for the redundancy. (N-K) units remain cold. When one or more units of K units, unit (s) of (N-K) will be replaced with failed unit (s). The

† 교신저자; 한국항공우주연구원 위성운용실
E-mail : yjcheon@kari.re.kr
Tel : (042) 860-2757, Fax : (042) 860-3909
* 한국항공우주연구원 영상운영지원팀
** 충남대학교 전자공학과
*** 한국항공우주연구원 다목적실용위성 3 호사업단

replacement will be done by either ground-command or on-board function, called on-board fault management (OFM).

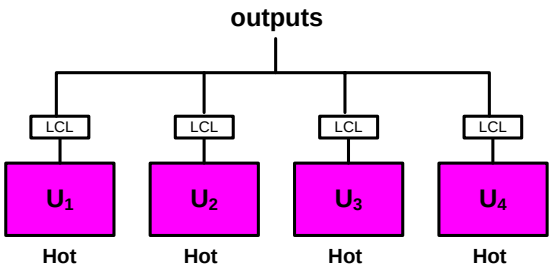

Figure 3 K of N Active Redundancy Architecture

2.3 Dual Active Redundancy

In dual active redundancy architecture, both units are equally operational for the same input and produce the same outputs. At least one unit supports system operations when one of dual units fails. The concept of either preemption or racing, or both can be applied for redundancy operations.

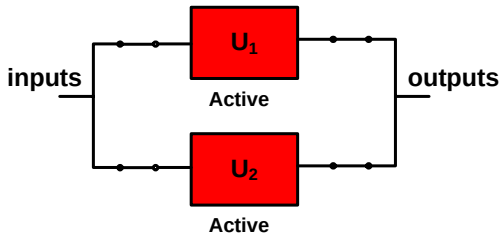

Figure 4 Dual Active Redundancy Architecture

2.4 Full Redundancy

If system adopts full redundancy architecture, units are freely selectable for primary units for supporting system operations. Non-selected units remain cold as a backup system in the events of anomalies or contingencies.

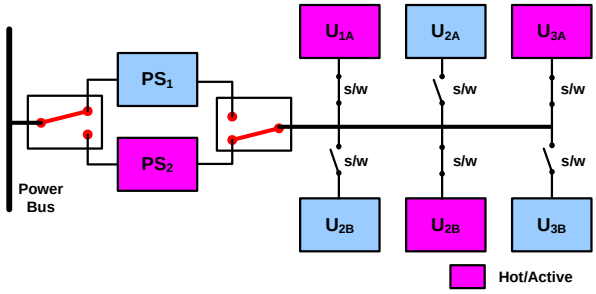

Figure 5 Full Redundancy Architecture

2.5 Hot/Cold Redundancy

In this architecture, either units on Side-A or ones on Side-B are single-strung. The design for system operations is very simple. If the current selected string fails, then the other string will be operational. Pros. for this architecture dramatically are cost reduction of design, test , and verification. Cons. are limitation of operational flexibility.

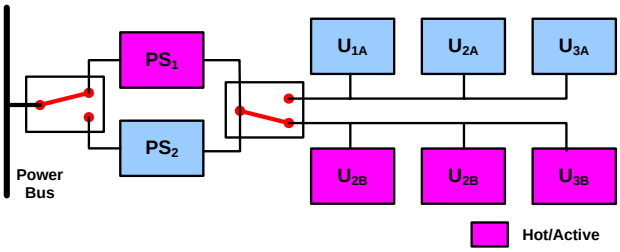

Figure 6 Hot/Cold Redundancy Architecture

2.6 Selective Redundancy

This architecture can be selected as a trade-off between full and hot/cold redundancy architectures in terms of costs and run-time reliability. It provides marginal operational flexibility and multiplicity for system operations.

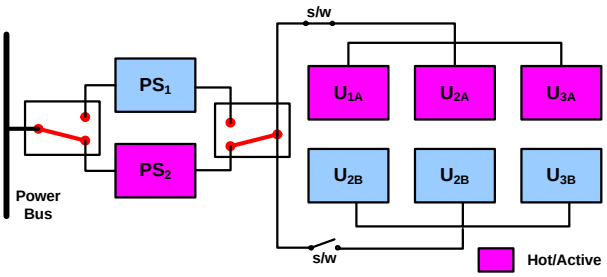

Figure 7 Selective Redundancy Architecture

3. Conclusion

This paper explores various design architectures for fault-tolerant satellite system with redundant units or subsystems. To ensure the system safety for anomalies or contingencies, the implementation of fault-tolerant redundancy architecture is required. However, for a real application of redundancy architecture, complexity or flexibility of system should be taken into account from either operational perspective or design one. In addition, costs such as budget, schedule and technical risk should be considered from programmatic perspective.