A Reliable Distributed Computing System Architecture for Planetary Rover

C. Jingping (1), J. Yunde (2)

(1) Department of Computer Science and Engineering, Beijing Institute of Technology, Beijing 100081, China, (2) Department of Computer Science and Engineering, Beijing Institute of Technology, Beijing 100081, China (caijp@bit.edu.cn / Phone: 86-10-68914849)

Computing system is one of the most important parts in planetary rover. Computing system is crucial to the rover function capability and survival probability. When the planetary rover executes some tasks, it needs to react to the events in time and to tolerant the faults cause by the environment or itself. To meet the requirements, the planetary rover computing system architecture should be reactive, high reliable, adaptable, consistent, and extendible. This paper introduces reliable distributed computing system architecture for planetary rover. This architecture integrates the new ideas and technologies of hardware architecture, software architecture, network architecture, fault tolerant technology and the intelligent control system architecture.

The planetary computing system architecture defines three dimensions of fault containment regions, the channel dimension, the lane dimension and the integrity dimension. The whole computing system has three channels. The channels provide the main fault containment regions for system hardware. It is the ultimate line of defense of a single physical fault. The lanes are the secondary fault containment regions for physical faults. It can be used to improve the capability for fault diagnosis within a channel, and can improve the coverage with respect to design faults through hardware and software diversity. It also can be used as backups for each others to improve the availability, and can improve the computing capability. The integrity dimension provides faults containment region for software design. Its purpose is to protect the critical component from the propagation of system errors.

The communication system has two networks. One connects the channels, and the other connects the lanes. The channel network uses intelligent network card. It can be configured to different communication mode. Every two channels have independent sending and receiving physical links, and any link failure does not affect the others. The lane network transmits the less real time data, and uses as the backup of the channel network.

The design of the software architecture mainly considers the analysis of functions, the different level computational abstractions, different processes and different methods, as well as the requirements of time, status and accuracy. The software architecture of the application includes the follow parts:

- Application Support Environment: It provides a consistent computing environment for the distributed applications. This Environment conceals the physical deployment of the distributed computing system, as well as the mapping from function modules to the computers. At the same time, it also provides the support to distribute fault tolerance.
- Functional Level: It is a level based on the elementary actions and perceptions. These elementary robot actions implement processing functions and task-oriented servo-loops, and perceptive capabilities. This level is made of a network of modules which integrates basic functions and servo-loops. The modules can communicate with each other and have no permanent layers.
- Execution Control Level: It controls and coordinates the execution of the functions distributed in the modules according to the task requirements and the states of the modules.
- Decision Level: This level is bases on the models. It includes the capacities of producing the task plan and supervising its execution. At the same time it reactive to events from the lower level.
- System Management Level: This level includes the capacity to manage and configure the application system, and manage the function of fault tolerance.

The simulating system is consisted of six industry computers. One channel includes two computers and they belong to the different lanes. The network system includes two 100M Ethernet. One connects the channels and the other connects the lanes. The system also simulates some relevant reliable communication and fault tolerant technologies. The research and simulating results prove that the distributed computing system architecture which combines the new technologies of intelligent control and fault tolerant is feasible and efficient, and can meet the needs of reliable computing system for planetary rover.