Implementation of the Fault Tolerance Module in PHOENIX CubeSat

Author: Li-Wei Chen, Te-Chuan Huang
Advisor: Jyh-Ching Juang,
Department of Electrical Engineering
National Cheng Kung University, Tainan, Taiwan
Outline

• Introduction
• Phoenix Nanosatellite
• Flight Software Design for Phoenix
• FDIR Module
• Conclusion
Introduction

- A **CubeSat** is a type of **Nanosatellite** (10x10x10 cm, weight 1 kg) which offers all the standard functions of a normal satellite.

- **Command and Data Handling System (C&DH):**
  - Schedule Mission Tasks
  - Payload Operation and Data Handling
  - House-Keeping
  - Ground Command Handling

Phoenix, 2U CubeSat
QB50 Mission

An international network of 50 CubeSats for multi-point, in-situ, long duration measurements and in-orbit demonstration in the lower thermosphere.

Images from VKI
Phoenix Nanosatellite

Payloads: 1. Ion and Neutral Mass Spectrometer (INMS)
2. Solar EUV Sensors
NanoMind A712D is a space proven COTS manufactured by GomSpace

- **Main Features:**
  - 32-bit ARM7 RISC CPU
  - Compatible with FreeRTOS
  - 2GB MicroSD card
  - I2C interface
  - USART interfaces
  - GPIO pins
  - Real Time Clock

Images from GOMSpace
Flight Software Feature

Task Scheduler

- Payload Operation Task
- Telecom Task
- House-Keeping Task
- ADCS Task
Failure Mode Analysis

**Hardware Issue**
- Hardware Damaged
- Single Event Upset (SEU)
- Single Event Latch-Up (SEL)

**Software Issue**
- Parameters changed by SEU
- Task Execution Failure
- Execute illegal Ground commands

**Human Factor**
- Set improper configuration on the CubeSat.
- Send improper commands..., etc.
Failure Mode Analysis

**Hardware Issue**
- Hardware Damaged
- Single Event Upset (SEU)
- Single Event Latch-Up (SEL)

**Software Issue**
- Parameters changed by SEU
- Task Execution Failure
- Execute illegal Ground commands

**Human Factor**
- Set improper configuration on the CubeSat.
- Send unauthorized commands... etc.

- **Software Isolation**
- **Power Reset**
- **Acceptance Check**
- **Define the margin for each parameter**
- **Authority Check**
FDIR Implementation

- Data Redundancy
- Watch Dog Timer
- Software Supervisor
FDIR Module Implementation

Data Redundancy

• To against Single Event Upset (SEU)
  - Cyclic Redundancy Check (CRC) algorithm in file-system
  - One additional backup copy
Watch Dog Timer

• As the final defense
• Against communication latch-up
  - Should be reset by software in a period
  - If somehow no one reset it, power reset the satellite.
Software Supervisor

- To against single events & Task Failures
  - Routinely scan important parameters
  - Reset watch dog timer
  - Supervise target tasks
  - Recover failure according to library
  - Generate error report
  - Library can be updated by uploading scripts
Supervisor Operation Flow

Activate by Task Scheduler

Work Tasks

Ex: HK task, Payload operation task..., etc.

Supervisor Tasks

Activate by Task Scheduler (option)

Ex: HK Supervisor, Payload Supervisor.
Supervisor Operation Flow

- Stage 1
- Stage 2
- Stage 3
- Stage 4
- Stage 5

Message Queue

First in, first out

Send S1 status

Get S1 status

Supervisor Tasks

- Check Stage 1
- Check Stage 2
- Check Stage 3
- Check Stage 4
- Check Stage 5

LOOP
Supervisor Operation Flow

- Stage 1
- Stage 2
- Stage 3
- Stage 4
- Stage 5

First in, first out

- Check Stage 1
- Check Stage 2
- Check Stage 3
- Check Stage 4
- Check Stage 5

If every thing goes well
Supervisor Operation Flow

- Check Stage 1
- Check Stage 2
- Check Stage 3
- Check Stage 4
- Check Stage 5

Hey, something is wrong!
Error Recovery Script

- Library can be updated by uploading scripts

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Stage</th>
<th>Error code</th>
<th>Solution ID</th>
<th>Solution command</th>
<th>Check sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Task ID</td>
<td>The failure stage</td>
<td>Describe the error type</td>
<td>The steps of solutions</td>
<td>Ex: Reboot a Subsystem, Configure Parameters, Power control</td>
<td>CRC16</td>
</tr>
</tbody>
</table>

2015/04/21 IAA 2015
Conclusion

• Three FDIR method are discussed here: Data Redundancy, Watch Dog Timer and Software Supervisor.

• SEU can be detected and corrected by Data Redundancy and Software Supervisor.

• Watch Dog Timer is the final defense.

• Solution library provides flexibility when dealing with failures.
10th IAA Symposium on Small Satellites for Earth Observation

THANK YOU FOR YOUR ATTENTION

mike6102@gmail.com
satellite.ncku.edu.tw