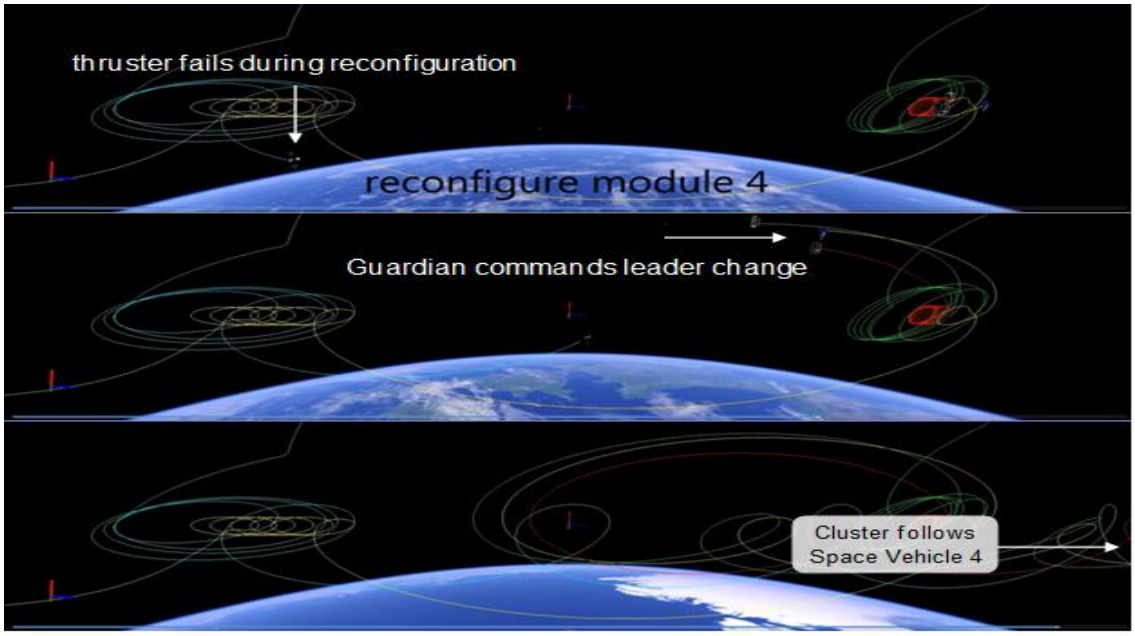
Guardian

FDIR

Fault detection isolation and recovery (FDIR) is one of the key technologies that enable distributed and disaggregated mission architectures, wherein multiple vehicles work cooperatively and autonomously in a cluster or formation, a typical mission concept involving small satellites. Guardian addresses the issues imposed by FDIR for decentralized systems with many coupled or loosely coupled subsystems such as a cluster of space vehicles implementing a service-oriented architecture and using a hierarchical design. Appropriate fault detection solutions can be selected from a library of interchangeable algorithms – the number and types of algorithms used would depend on the application of the fault management architecture, and higher-level isolation and recovery services can be easily configured to implement new health information provided by new fault detection services. This promotes easy adaptation to new systems and future missions such as unmanned vehicles, cloud servers, and networks of biomechanical devices. The hierarchical design of Guardian addresses the challenge of fusing FDIR results from many different subsystems that may be distributed among a cluster, which is loosely defined as multiple independent modules, or systems of systems, connected via intermittent communications. The architecture defined by Guardian allows expedient FDIR on a single spacecraft, or any other type of independent module, while promoting robust FDIR solutions across the cluster of modules. The well-defined structure clarifies service roles for engineers new to Guardian, and it eases the burden of verification and validation for the integrated system.

Specifications

- Linux OS
- 10MB disk space for executables and configuration files
- ARM and x86 processors
- Consumes health information from other software systems
- Publishes health telemetry
- Commands recovery actions in response to detected change in health
- GEAR integration
- Provides fault detection, isolation, and recovery services enabling autonomous operations



Modules/Components

Recovery

- Distributes system requirements among components with well-defined interfaces and functionality. Defines decentralized roles for components. Enables extension, reuse, and verification of functionality.

Diagnosis

- Fault isolation and recovery services are configurable enabling reuse for future mission architectures. Existing detection modules from previous mission deploy quickly to new missions.

Navigation Monitor

- Navigation Monitor implements two fault detection algorithms: Receiver Autonomous Integrity Monitoring (RAIM) of GPS pseudorange measurements. RAIM is a proven algorithm for GPS solution integrity monitoring that detects pseudorange measurements instead of GPS.

Cluster Monitor

- For our multi-spacecraft GN&C problem, two cluster-level fault detection algorithms were implemented in Cluster Monitor that utilize the parity between GPS and range measurements. The filter/range parity algorithm uses relative range measurements to verify the navigation estimate by comparing the measured relative ranges of the spacecraft with the expected ranges based on the estimated positions from the navigation filter. A second algorithm, receiver autonomous integrity monitoring augmented with relative range measurements, operates when there are more than the minimum of four GPS range measurements, like the RAIM algorithm does, and augments RAIM by including the GPS ranges for all the spacecraft in the cluster and relative ranges between the spacecraft.

Thrust Monitor

- Thrust Monitor detects faults in the onboard thrusters. To determine if there is a fault, it compares measurements from the accelerometer to the expected acceleration caused by the nominal command thrust. It also evaluates fault modes, such as loss of effectiveness (LOE) or stuck thruster, by comparing the acceleration measurements to the accelerations expected in those fault modes.

Crosslink Monitor

- Crosslink Monitor determines health of crosslink communications by monitoring navigation solution messages from other space vehicles.