Components, Partitions, Networks: Our Approach to use IMA Principles in Spacecraft On-board Applications

Prochazka, M.; Lopez-Cueva, P.
SciSys

Integrated Modular Avionics (IMA) addresses various technical aspects of aircraft systems hosting multiple software modules certified to different criticality levels. SciSys have been active in pursuing IMA principles in its recent spacecraft on-board software research projects. This is reflected by three key goals: 1) Systematic building of software from well specified building blocks with improved support for reuse and incremental design, static and dynamic reconfiguration, and composition; 2) Integration of different communication protocol and physical networks, as well different types of devices; 3) Support for both static and runtime mechanisms to enable secure sharing of resources amongst applications with different criticality levels.

In the DisCo project we have proposed Space-Oriented Middleware (SOM) which provides support for application distribution as well as a broad set of services. A part of the SOM is an application framework which allows in a uniform way to control application lifecycle, component update and configuration. In the COrDeT project we aim at enhancing our application framework to add more support for component composition as well as static and dynamic reconfiguration. We have also been taking part in the ASSERT project where correctness-by-design techniques have been implemented.

SciSys have been actively contributing to the group of SOIS standards which aim at defining generic services for simplifying the way flight software interacts with flight hardware and pursuing interoperability and reusability. In various projects such as ASSERT, DisCo, MARC, PRISM, etc. we have been implementing different parts of the SOIS standards for different hardware and RTOS platforms and testing their suitability to deal with on-board application requirements.

One of our key interests is the support for applications with multiple levels of criticality. In DisCo, this has been reflected by several design and architecture principles:
1) Support for CPU-time monitoring at runtime. We have used hierarchical scheduling to support temporal partitioning. Our first-level scheduler uses CPU-Time Timers in RTEMS to ensure that CPU budgets of applications are not exceeded. Our partition scheduling is more flexible and dynamic comparing to ARINC 653.
2) The SOM support spatial partitioning through the Information Flow Authorisation Service and resource pooling. However, the target LEON 2 architecture does not provide enough memory management support to allow us to provide full spatial isolation.
3) Our Communication Service (a part of the the SOIS Subnetwork layer) provides guarantees as to how much data is sent by different application per a period of time. This is achieved by assigning bandwidth quotas to applications.

In the ASSERT project temporal isolation between different partitions is ensured by means very similar to those used in the DisCo project. In addition, thanks to generating the low-level application code, most of the isolation properties are guaranteed statically instead of relying on runtime checks.

In summary, SciSys have been involved in several projects dealing with IMA applied to spacecraft on-board applications. We have developed technologies supporting component-based software engineering approach, combining different communication protocols, networks and devices, as well as supporting temporal, spatial and communication partitioning.