FDIR Handling in Eu:CROPIS ACS

Olaf Maibaum (1), Ansgar Heidecker (2), Fabian Greif (2),
Markus Schlotterer (2), Andreas Gerndt (1)
(1) German Aerospace Center (DLR), Simulation and Software Technology, Lilienthalplatz 7, 38108 Braunschweig, Germany
(2) German Aerospace Center (DLR), Institute of Space Systems, Robert Hooke Str. 7, 28359 Bremen, Germany

Fault detection, isolation, and recovery (FDIR) mechanisms in the on-board software are essential to guarantee the survival of the satellite in case of a hardware malfunction. E.g., outage of essential attitude control system (ACS) actuators or sensors can lead to mission loss. The on-board software has to handle such situation autonomously by switching to cold redundant devices or by isolation of information from hot redundant devices. The paper will show the implemented software mechanisms and methods for FDIR handling in the Eu:CROPIS (Euglena Combined Regenerative Organic food Production In Space) ACS.

After a short description of the Eu:CROPIS satellite bus and the ACS, the paper introduces the used packet utilization standard (PUS) services for FDIR handling. These are the following services: device command distribution (PUS-Service 2) to parametrize the system, diagnostic data reporting (PUS-Service 3) for regular and extended telemetry data, event reporting (PUS-Service 5) to report events, and function management (PUS-Service 8) to initiate special processing. The communication and processing of tasks is realized in the ACS by the Tasking framework. With the Tasking framework, a task is performed when data is provided on a channel declared as input of the task. The channels are the mean to communicate between tasks.

The FDIR handling in the Eu:CROPIS ACS has several logical layers. On the lowest layer of ACS actuator and sensor software interfaces, the communication with the device and status information from the device is observed. In case of a detected failure, an error identification is send on the error channel. Depending on the failure, device information are blocked or sent with a failure state information to the ACS controller layer via corresponding data channels. In the ACS controller layer, the sensor and actuator data is filtered by an unscented Kalman filter. Inaccurate sensor and actuator data are isolated in the filter and, under some fault conditions, the controller can also send an identification of the fault to the error channel. Information on the error channel is cooperatively read by two ACS tasks: one task initiates the sending of diagnostic data, the other task manages ACS error counters. The diagnostic data sent is a serialization of data from a set of channels related to the error identification, e.g. in case of an failure of the magnetic torque, all channels related to the sender and receiver task of the magnetic torquer software interface are serialized to a diagnostic data package. The error counter management task decides on basis of the error counters state and the criticality of the error whether an error should be propagated as event to the bus system. On bus system level, an FDIR state machine observes the reported events from all subsystems and reacts on it by state switches and actions like switching the power state to cold redundant devices. The implementation details and ways to maintain and operate the FDIR handling will be shown in the paper.