Project: Generic AOCS/GNC Techniques & Design Framework for FDIR

Title: Executive Summary

Doc. No.: GAFE-RP-D7.2
Issue: 1.0
Date: 04.05.2018

	Name	Institution	Signature	Date
Author(s):	Domenico Reggio	Airbus Defence and Space		
	Patrick Bergner	Airbus Defence and Space		
	Marc Hirth	Astos Solutions		

DISTRIBUTION LIST

Quantity	Type	Name	Company/Department
1	PDF	Alvaro Martinez Barrio	European Space Agency, ESTEC
1	PDF	Marcel Verhoef	European Space Agency, ESTEC
1	PDF	Guillermo Ortega	European Space Agency, ESTEC
1	PDF	Study Team	Airbus DS GmbH, iFR Universität Stuttgart, Astos Solutions GmbH

CHANGE RECORD

Issue	Rev.	Date	Pages/Section	Changes
1	0	04.05.2018	All	Initial Issue

TABLE OF CONTENTS

1 Introduction

This document gives a brief overview of the activities performed in the GSTP study "Generic AOCS/GNC techniques and design framework for Failure Detection, Isolation and Recovery" conducted by Airbus Defence and Space under contract of the European Space Agency (Contract No.: 000112992/14/NL/MH). Subcontractors were Astos Solutions GmbH and iFR (University Stuttgart).

The main objectives of the study were the elaboration of a methodology for the design and early validation of the AOCS/GNC Failure Detection, Isolation and Recovery System for spacecraft, and the design and implementation of a software framework to support these tasks. Together, the Methodology, the Structural Analysis and the Simulator form the GAFE Framework.

Technical officer for the study on ESTEC side was Alvaro Martinez Barrio, with valuable support from Marcel Verhoef.

1.1 Reference Documents

Reference Documents

[RD-1] GAFE User's Manual, GAFE-UM-D7.5a, Issue 1.0

[RD-2] GAFE Methodology, GAFE-UM-D7.5b, Issue 1.0

[RD-3] Generic FDIR Design for each Mission Scenario, GAFE-RP-D1.1, Issue 1.2

[RD-4] Terms & Definitions, GAFE-LI-1001, Issue 1.2

2 Review of FDIR Design of Existing Missions

The starting point of the GAFE study activities was the critical review of the fault management concept of several space missions. The focus was set on the FDIR requirements, FDIR architecture & design, the FDIR engineering process, the tools used and the lessons learned from development and/or in-flight experience.

All reviews performed and the output collected was structured identically (see [RD-3]):

- Mission overview incl. constraints
- Important mission requirements (on customer and system level)
- Electrical and AOCS/GNC architecture, incl.
  - AOCS/GNC modes
  - Installed equipment
  - Redundancy concepts
- FDIR architecture, design and implementation
- FDIR Verification and Validation
- FDIR engineering
  - General approach
  - Responsibilities
  - Used methods
  - Applied process.
  - Lessons learned (positive & negative, from development and in-orbit experience)
- Collection of key parameters for a rough comparison using a common metric

The following missions from different categories have been reviewed in detail:

- Rendezvous & Docking: ATV
- Extraplanetary Science: BepiColombo, Rosetta
- Earth Observation & Science: Sentinel 2, Grace FO, SWARM, MTG
- Formation Flying: TanDEM-X

Additional reviews have been performed for Ariane 5 (launcher) and IXV (re-entry). Their outcome was limited, because no sufficient documentation was accessible or available in time.

The outcome of the mission reviews was a synthesis of the gained insights, which were used as a foundation for the next tasks of the study, i.e. the definition of the GAFE Methodology and the GAFE framework. In addition, the most important terms and definitions in the context of fault management & FDIR have been collected and consolidated (see [RD-4]).

3 GAFE Methodology

The GAFE Methodology describes the FDIR design and development process for the AOCS/GNC of a spacecraft. Its starting point is the nominal AOCS design. The methodology is supported at key points by the GAFE Structural Analysis and GAFE Simulator.

The FDIR Methodology is subdivided in seven main tasks:

- Analysis of the fault management requirements (Task #1)
- Extension of nominal AOCS equipment set (Task #2)
- Definition and implementation of FDIR concept (Task #3)
- Customization & Parameterization of the FDIR Simulator (Task #4)
- Definition & Simulation of Test Cases (Task #5)
- Evaluation of FDIR performance (Task #6)
- Generation of FDIR documentation (Task #7)

These seven parts are illustrated by the dashed boxes in the linear representation of the high level flow in Figure 3-1. The orange bars indicate parts with are supported by the tools of the GAFE Framework. Tasks 1 to 3 comprise the conceptual FDIR design and are assisted by the GAFE Structural Analysis. Tasks 4 to 7 cover the early verification and validation of the FDIR; these tasks required the use of time domain simulation tools like the GAFE Simulator.

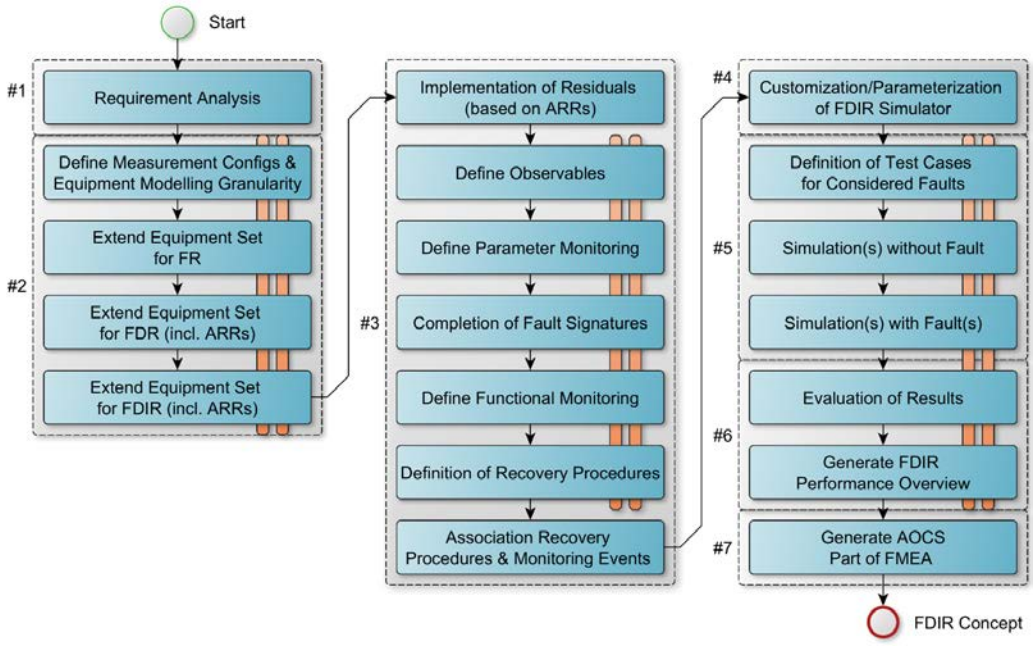

Figure 3-1 High level flow of GAFE Methodology for AOCS FDIR design and V&V.

A more detailed representation of the flow, which also distinguishes between inputs, tasks, intermediate results and decisions, is given in [RD-2]. In contrast to the linear representation it shows also the return path to entry points in case iterations are required.

The main items contained in each task are:

- Analysis of the fault management requirements (Task #1)
  - Failure tolerance requirements
  - Availability requirements (typically related to fail-operational failure recovery)
  - Best-practice requirements
  - Reliability requirements
  - Survivability requirements (typically related to fail-safe failure recovery)
- Extension of nominal AOCS equipment set (Task #2):
  - Achieve compliance to failure tolerance requirement in terms of recovery
  - Achieve compliance to failure tolerance requirement in terms of failure detection
  - Achieve compliance to availability requirements
- Definition and implementation of FDIR concept (Task #3):
  - Definition of observables, parameter & functional monitors, recovery actions
- Customization & Parameterization of the FDIR Simulator (Task #4)
  - Environment & Dynamics: orbit, time, environmental models, spacecraft properties, …
  - Spacecraft: AOCS equipment, alignment, sizing, operational states, …
  - AOCS algorithms (nominal and for FDI)
  - System level aspects: system configuration(s), AOCS modes, mode transition, required equipment configuration per mode
  - Faults: which faults shall be considered
  - FDIR: All kind of monitors and response actions.
- Definition & Simulation of Test Cases (Task #5)
  - Scenario definition, fault free case, faulty case (with and without recovery action)
- Evaluation of FDIR performance (Task #6)
  - Detection performance, isolation performance, time for recovery
- Generation of FDIR documentation (Task #7)
  - Aggregated information can be used to create main part of AOCS FMEA

4 GAFE Structural Analysis

The GAFE Structural Analysis Tool is one part of the GAFE Framework. It is based on a mathematical method called "structural analysis". This method focusses on structural relations between known and unknown "states" of a system and allows to identify if it is possible to detect and/or isolate (unambiguously identify) faults in predefined elements of the system.

Examples for such structural modes are given in Figure 4-1. A general introduction into the method itself is given in [RD-2], Appendix A.

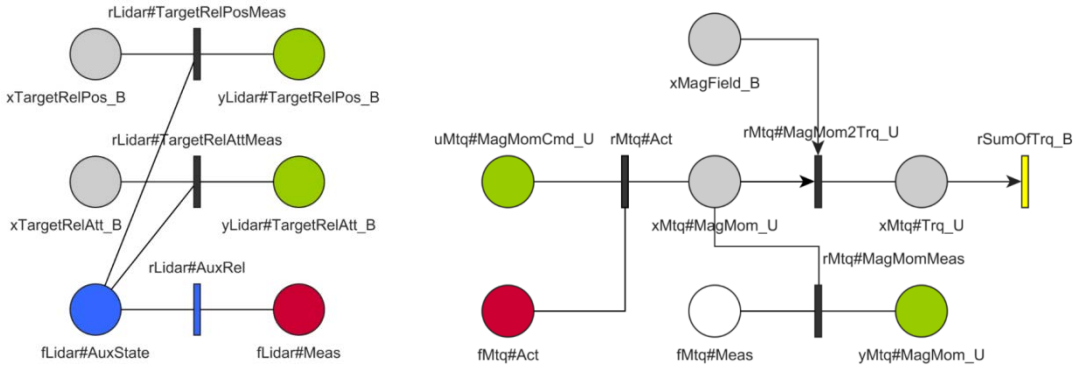

Figure 4-1: Examples for structural models (here of a LIDAR and a magnetometer).

The purpose of the GAFE Structural Analysis Tool is to assist the user in the extension of nominal AOCS equipment set and in parts of the FDIR concept definition. The extension of the nominal equipment set has the goal to make the set compliant with the required fault diagnosis capabilities (i.e. fault detection and potentially isolation for all considered faults) and the requested failure tolerance requirement (fault recovery) for all AOCS modes. In general this task consists of adding or activating additional AOCS units and/or analytic redundancy models. The outcome of this task is the extended equipment set for failure detection (, isolation) and recovery (EES-FDR/FDIR).

In contrast to the manual and sequential approach of adding or activating single additional AOCS units and/or analytic redundancy models until the required diagnostic capability (fault detection for fail-safe, fault detection and isolation for fail-operational) for all AOCS modes is achieved, the GAFE Structural Analysis Tool performs this task in a structured and automated way. Besides that it allows the user to defined a cost function (in terms of price, mass, power consumption and CPU load, e.g. for sensor processing or analytical models) for which well suited solutions are searched. The high level workflow of the structural analysis is sketched in Figure 4-2.

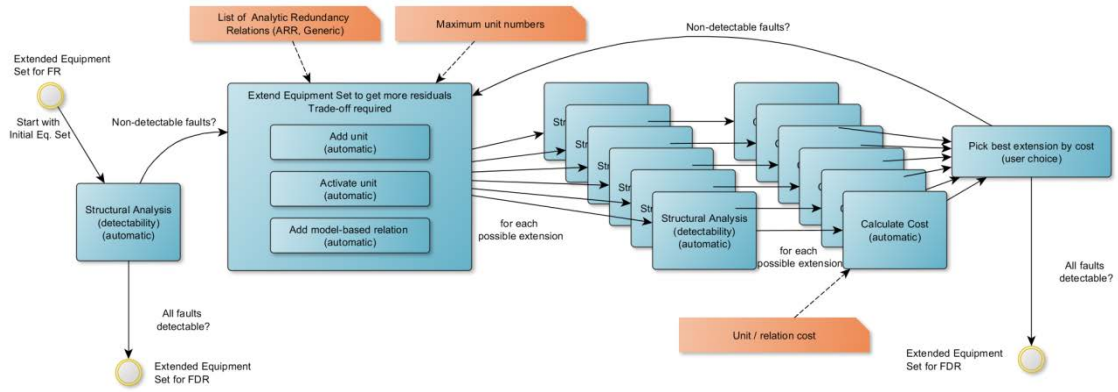

Figure 4-2 High level workflow of GAFE Structural Analysis for automatic extension of nominal AOC Sequipment set.

The result of the structural analysis consists of an overview of the investigated solutions (e.g. in terms of cost, see Figure 4-3), of the AOCS equipment set to be integrated in the spacecraft, the subsets of this equipment to be active for the different AOCS modes, the required analytic redundancy models for FDIR purposes, the residuals to be computed onboard and the fault signatures required for the identification of the considered faults.

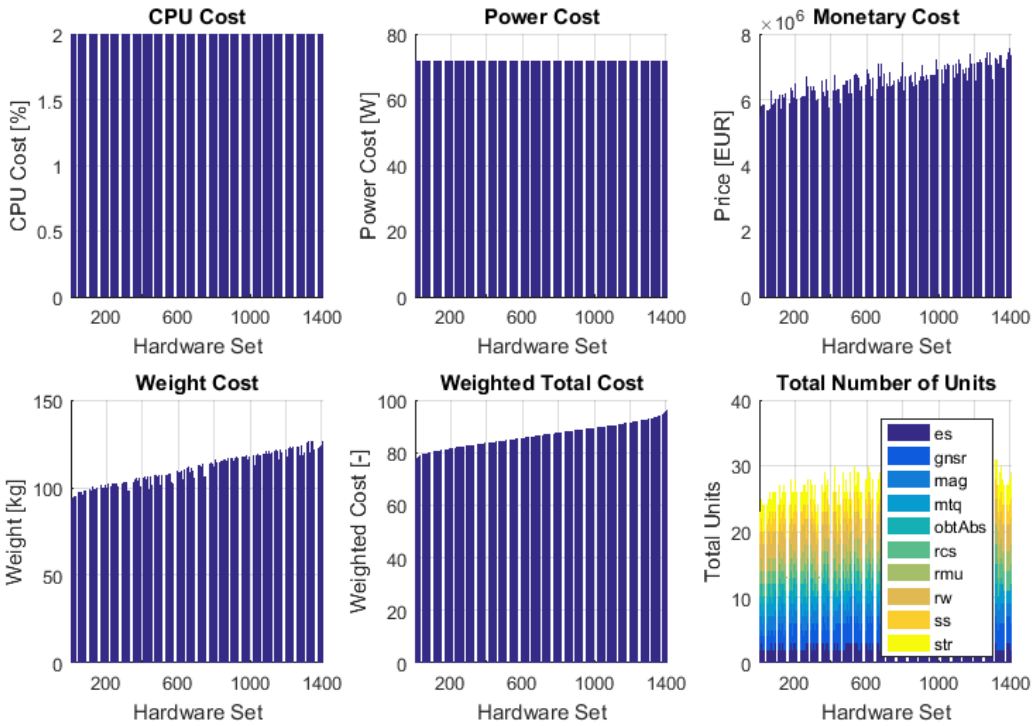

Figure 4-3 Cost overview of solutions obtained by GAFE Structural Analysis.

5 GAFE Simulator

The GAFE Simulator is an AOCS/GNC time domain simulator with special focus on FDIR related aspects. It supports well the GAFE methodology by enabling the early verification and validation of the FDIR design. It allows a quick implementation of the outputs of the structural analysis, together with a preliminary set of AOCS algorithms, FDIR/OPS and functional system behaviour.

The GAFE Simulator has the following main characteristics, which fit the needs of FDIR design, implementation and validation:

- Uses outcome of Structural Analysis in form of functional behaviour and terminology
- Focus on FDIR behaviour throughout all interactive parts: Equipment, AOCS Algorithms, PUS Services, System (Configuration, Equipment Management, AOCS Mode Management)
- Fully data-driven configuration, including
  - System, FDIR/OPS, AOCS Algorithms configuration
  - Equipment instantiation (number of units and their individual parametrisation)
- Provides libraries for
  - AOCS Algorithmic Components
  - Equipment (Actuators, Sensors, Non-AOCS devices)
- Programmers interface for new AOCS Algorithmic Components and new Equipment
- Full observability and logging of all relevant information
- Logging data preconditioning and visualisation
- Monte-Carlo capability with ready to use parameter variation concept

The breakdown into Modules and their main tasks in the frame of FDIR gives a good overview about the included functionality:

- System
  - System Configuration Manager
    - manages current system configuration (system state, processor module, avionic chain) from a list of possible (user defined) system configurations
    - Distribution of information to Equipment Manager, AOCS Mode Manager, AOCS Algorithms, FDIR/OPS
    - models reboot delay of the on-board computer
    - defines initial AOCS mode and Equipment power cycling at wake-up
    - defines source and usage of context information
    - enables/disables FDIR
  - Equipment Manager
    - selection and activation/deactivation of AOCS units currently required

        - keeps unit's health status
        - informs about overall status of equipment required for current and desired AOCS mode
    - AOCS Mode Manager
        - manages AOCS main modes and submodes
        - gets inputs from OPS PUS Services (monitoring positive AOCS Algorithms flags) and from ground (TCs)
        - distributes to Equipment Manager, FDIR/OPS and AOCS Algorithms
- FDIR/OPS PUS Services model
    - parametrises Parameter Monitors, Functional Monitors, Event Actions with the same content and behaviour as the real PUS Services (12, 142 (private), 19, 5)
    - applied for FDIR purposes
    - slightly enhanced to be also used for OPS (!) purposes (e.g. for switching AOCS modes)
- AOCS Algorithms
    - gets HK inputs from Equipment
    - is subdivided into AOCS Algorithmic Components which defines modularity
    - follows standardized interface and design rules for Components
        - provides standard validity flags from one Component to the next to allow clear functional chains and blocks propagation of “problems”
        - each Component delivers its specific status information about invalidities, checks and positive events (used by FDIR/OPS)
        - clean and simple way to declare and set states
    - generates overall AOCS Algorithms automatically based on user parametric configuration of Components handling
        - Components activation/deactivation for specified modes
        - Components handling of sample rates and offset, outputs and states hold and reset
        - Overall states handling to allow context information usage driven by System
    - provides this preset of AOCS Algorithmic Components
        - Measurement processing for: Magnetometer, Earth Sensor, Sun Sensor, Startracker, GNSR, Lidar, Camera, Clock, Reaction Wheels
        - Determination functions for: Satellite attitude and rate, Earth direction, Sun direction, Magnetic field and rate, Orbit (OOP), Earth ephemeris, Relative position and orbital elements (to target), Reaction Wheel friction estimation, ...
        - Controller for: Rate Damping, Attitude Acquisition and Safe Mode, Nominal Mode, ...

        - Actuator Commanding for: Magnetorquers, Reaction Wheels, Reaction Control Systems (Thrusters)
- Equipment Models subdivided into
    - Generic model part common to all equipment types
        - Mini-State-Machine (on,off,full performance, degraded performance)
        - Error injection (stale data, drift, noise increase, bias, …)
    - Specific part, belonging to a certain type of AOCS equipment:
        - with the specific algorithm for the main functionality of this equipment
        - Sensors available: Magnetometer, Earth Sensor, Sun Sensor, Startracker, GNSR, Lidar, Camera, Accelerometer, Clock
        - Actuators available: Magnetorquer, Reaction Wheels, Reaction Control System (Thrusters)
        - Additional: Solar Array Drive Mechanism (SADM), Antenna Pointing Mechanism
- Classical Environment simulation with
    - Position and Attitude Integrators
    - Earth rotation, Equation of equinoxes and time, Nutation, Precession
    - Gravity and Magnetic field model of higher order
    - Different atmospheric models, Solar pressure, Gravity disturbance of Sun and Moon, Gravity gradient, Residual magnetic moment
    - Satellite modelling as point or as sphere or with faces
    - Using Terrestrial time (TT) and UTC

The top-level architecture with the Modules described above can be found in Figure 5-1.

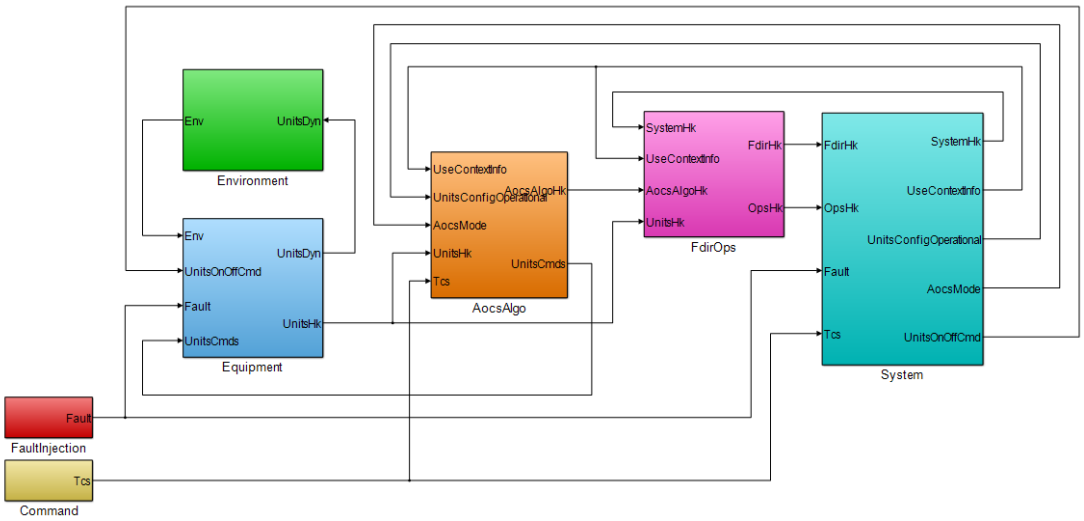

Figure 5-1 Top-level architecture of GAFE Simulator.

After running simulations (single ones or in batch mode), the logging data is made available for further post-processing and detailed inspection.

The picture below visualizes a typical session for visualization and inspection:

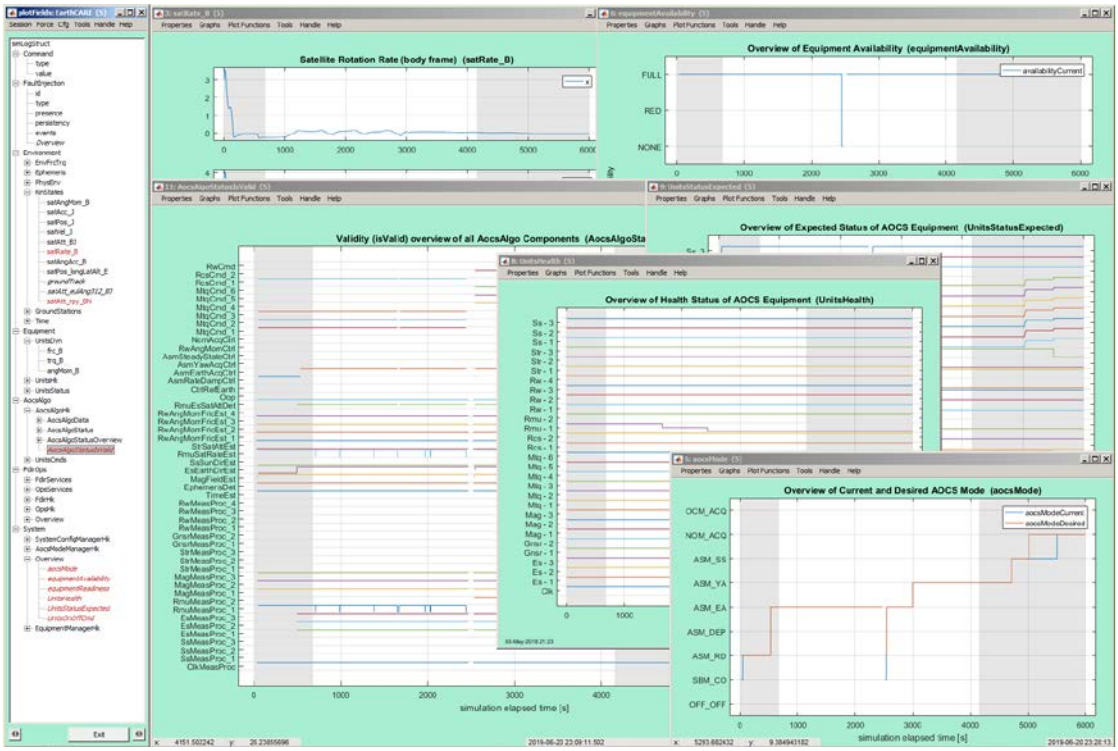

Figure 5-2 Visualization of typical simulator output for inspection.

6 Re-Enginering Study Cases

Two study cases have been selected to apply the developed GAFE Methodology and Tools to.

The selected study cases were based on the existing projects:

- EarthCARE – an ESA project currently in phase D
- e.Deorbit – an ESA study still in early phase

These two study cases had multiple goals

- Demonstrate that the methodology can be applied within an acceptable amount of effort and time
- Demonstrate that the output of this study case bring added value to the projects if applied early
- Validate the framework by comparison to the already existing results in the real project

The re-engineering process for each project was structured in the following way:

- Overview of existing mission in terms of:
  - Main objectives, AOCS modes and mode transitions, required AOCS equipment, redundancy concept for AOCS equipment
- Overview of the study case in term of
  - Scenario definition, covered AOCS modes and mode transitions, required AOCS equipment
- Re-engineering process guided by GAFE methodology

The obtained results from the re-engineering were quite interesting. On the one hand they confirmed several design and implementation aspects of the FDIR implemented in the projects, on the other hand there were also interesting discrepancies. For EarthCARE e.g. obtained equipment set contained a different number of units for 4 equipment types. The differences could be traced back to a mixed concept regarding detectability and isolability of faults in the different AOCS modes.

Regarding the use of analytical models for FDI purposes the re-engineered solution for EarthCARE (main focus on hardware redundancy, analytical models only for equipment) was very close to the project.

The solution for e.Deorbit (were a detailed model-based FDI solution was not yet elaborated), showed many interesting options for fault detection and isolation supported by analytical models. Examples are the proposed inter-equipment cross-checks between LIDAR & Camera, GNSR, SS & STR, STR & RMU and RCS & RMU.

7 Conclusion of FDIR Engineering using GAFE

The benefit of the systematic approach for the AOCS FDIR design exercised with the GAFE methodology and tools can be seen on these study cases. The re-engineering approach required only a bare minimum of well-structured information to describe the FDIR design:

- Which units to monitor at which rate and on which levels, e.g.
  - power level,
  - communication level,
  - measurement processing level,
  - inter-unit cross-checks
- Which unit configurations are allowed in which AOCS mode
  - This point includes already the complete definition of any local unit reconfiguration!
- Which configurations are available on system level
  - avionic chain, context information use, initial AOCS mode, power cycling of units.

If the concepts of the System Components and the Algorithms are once documented, the whole FDIR design of a new project is technically fully documented by a few parameter files:

If the AOCS FDIR of the study cases would have been modelled in full detail, the amount of information would have grown. Nevertheless, the structure of information would have been exactly the same. This is the benefit of the in concepts and the systematic approach provided by the GAFE methodology and tools.

Another positive experience is not visible from the presented results of the study cases. It is the process to come to the details of the FDIR design.

During the re-engineering activities, several times FDIR effects were observed, which needed further investigation: Why is this flag, monitor or even action triggered? Why at this time?

Once understood, these observations led often to different monitoring limits, intervals or even completely modified checks of the parameter or functional monitors or modified recovery actions.

Acquiring this knowledge in an early project phase and being able to iterate the FDIR design as quickly as the GAFE framework allows, is real added value. So far this level of detail was available only in much later project phases, which made any iteration slower and more expensive. The consequence of the last two points is that in this case the FDIR is tested less extensively as it should be.