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

# Title: GAFE Methodology

Doc. No.: GAFE-UM-D7.5a
Issue: 2.0
Date: 13.06.2018


| | Name | Institution |
|---|---|---|
| Author(s): | Patrick Bergner | Airbus Defence & Space |
| | André Posch | Universität Stuttgart, iFR |
| | Domenico Reggio | Airbus Defence & Space |

# 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 | Study Team | Airbus DS GmbH,<br>iFR Universität Stuttgart,<br>Astos Solutions GmbH |

# CHANGE RECORD

| Issue | Rev. | Date | Pages/Section | Changes |
|---|---|---|---|---|
| 1 | 0 | 29.04.2018 | All | First Issue. |
| 2 | 0 | 12.06.2018 | 2.0 | Updated according to feedback of “Final Review”. |

# TABLE OF CONTENTS

# 1 Introduction

## 1.1 Scope of the Document

*This document presents a methodology for the design, development and validation of the fault management concept for the AOCS of a spacecraft. It is focused on early mission phases (preliminary design) and includes a high level overview of the process tasks and detailed procedures for the most important steps. The major points covered are the analysis of the fault management requirements, the extension of the nominal AOCS equipment set in order to make it compliant to the failure tolerance and availability requirements, and the definition of the onboard failure detection, isolation and recovery concept. At many points the tasks are supported by lists of items to be checked or considered, e.g. a list of best practice FDIR requirements and feared events, a condensed list of in-orbit failures of AOCS equipment, and typical parameters to be made available to the on-board monitoring. The methodology presented in this document is suitable for the class of single failure tolerant spacecraft, which is the most common class for unmanned missions. The methodology is closely linked to the GAFE Framework, which was developed side-by-side with the methodology. Several analysis steps and concepts discussed in this document are reflected in tools and concepts of the framework. It is therefore recommended to read first this document and to continue then with the User's Manual of the GAFE Framework.*

*The appendix to this document contains an introduction to the analysis method "structural analysis", which is very well suited for the detectability and isolability analysis required in the extension of the nominal AOCS equipment set. It also contains a section with abbreviations and the terms & definitions used in this document.*

*The generic approach of the GAFE methodology & framework presented in [RD-3] and in this document is independent of a specific type of spacecraft or mission.*

## 1.2 Reference Documents

[RD-1] GAFE User's Manual, GAFE-UM-D7.5b, Issue 2.0

[RD-2] NASA Fault Management Handbook, NASA-HDBK-1002, NASA, Draft 2, 02.04.2012

[RD-3] GAFE Framework Architecture, GAFE-DD-D3.2, Issue 1.0, 11.7.2016

[RD-4] ECSS-Q-ST-30-02C, Failure modes, effects (and criticality) analysis (FMEA/FMECA), 6 March 2009

[RD-5] Fault Diagnosis utilizing Structural Analysis, Mattias Krysander, Mattias Nyberg, Department of Electrical Engineering, Linkoping University, CCSSE_02_MKMN.pdf

[RD-6] Diagnosis and Fault-Tolerant Control, Blanke et al., Springer-Verlag, 2006

[RD-7] Catalogue of Failure Data for Safety and Dependability Analysis, V2.2.1

[RD-8] Assessment of the Methodology, Processes and Tools, GAFE-RP-D1.2, Issue 1.1, 13.06.2018

## 1.3 Fault Management Strategies

According to the differentiation in [RD-2] there are two main branches of fault management strategies: failure prevention and failure tolerance (see Figure 1-1). Failure prevention encompassed all tasks and means to ensure that failures will not occur. This branch can be subdivided into:

- Fault Avoidance: At design-time, stricter quality assurance processes, higher quality parts, or increased margin
- Failure Avoidance: During operation prevent failure from happening, e.g. through repair, replacement, or operational changes that reduce the failure's probability or delay its occurrence

The second branch is called failure tolerance and is concerned with how to mitigate or accepted the effects of failures that occur. This branch can be subdivided into:

- Goal Change: Allow failure to compromise system function, respond by changing the system's goals to new, usually degraded goals that can be achieved
- Failure Masking: lower level failure may occur, effects are masked, no effect on high level system function
- Failure Recovery: Allow a failure to temporarily compromise the system function, but respond and recover before the failure compromises a mission goal

The methodology presented in this document focusses on the failure tolerance branch, and there mainly on the typical FDIR domains of failure masking and failure recovery.

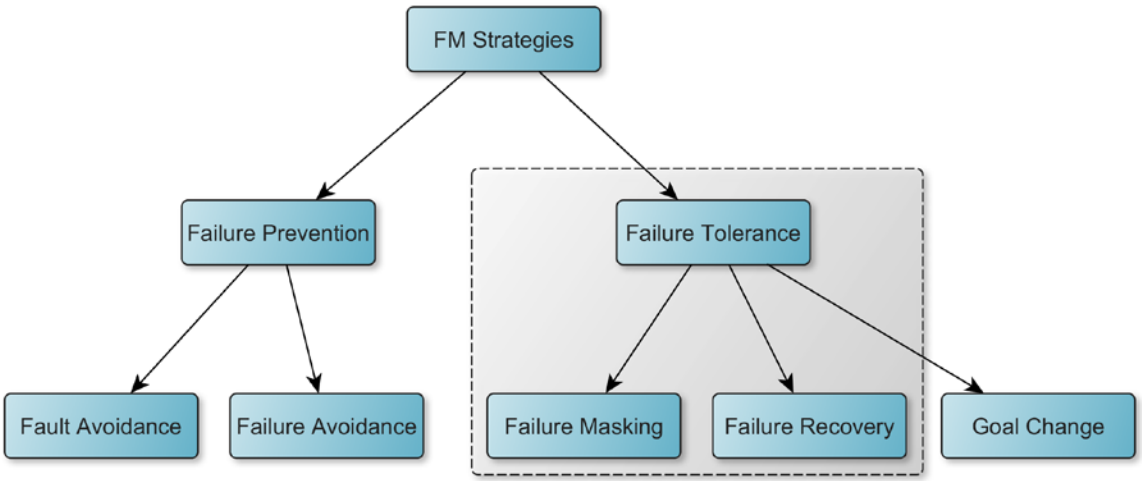


Figure 1-1 Hierarchy of Fault Management strategies according to [RD-2]. The dashed box highlights the items the methodology is focused on.

# 2 Required Inputs for FDIR Development Process

*For the development of the FDIR concept of an AOCS[1] a strict distinction should be made between the elements of the nominal AOCS design (i.e. such that are required to fulfil all functional and performance requirements in the absence of faults) and the elements required for the detection and isolation of faults and failures and the recovery of the system, either into a modified operational state or a non-operational, but safe state. This distinction does not only make design decisions and their justifications more transparent but also allows a clear separation of the responsibilities for tasks belonging to the nominal AOCS and the AOCS FDIR. The following section describes the elements of the nominal AOCS design, which is considered the starting point of the AOCS FDIR Design.*

## 2.1 Nominal AOCS Design

The *Nominal AOCS Design* comprises all items required to fulfil the functional and performance requirements of the AOCS in the absence of faults. It is assumed to be an input to the development of the AOCS FDIR and consists of:

- AOCS Mode Design
  - AOCS modes & submodes
  - AOCS mode transition table (see Table 2-1)
  - Mode transition conditions for all automatic (sub)mode transitions
  - Maximum nominal duration of all (sub)mode transitions
- Nominal equipment sets for all AOCS modes (see Table 2-2 and Section 2.2)
- Unit unavailability vectors (UUV) for all AOCS modes (see Section 2.2.2)
- Functional and performance requirements for all (sub)modes
- AOCS Safe Mode(s)
- AOCS Algorithm Design for each (sub)mode
  - Sensor processing functions
  - Determination functions
  - Guidance functions
  - Control functions
  - Actuator commanding functions

[1] When the term *AOCS* is used in this document, it stands at the same time for *GNC-system*.

Table 2-1: Exemplary AOCS mode transition table (M = Manual, A = Automatic).

| To AOCS Mode/Submode | | | From AOCS Mode/Submode | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | Mode1 | | | Mode2 | | Mode3 | |
| | | | Sub-ModeA | Sub-ModeB | Sub-ModeC | Sub-ModeA | Sub-ModeB | Sub-ModeA | Sub-ModeB |
| | Mode1 | SubModeA | (M)* | M | M | M | M | M | M |
| | | SubModeB | A | (M)* | | | | M | |
| | | SubModeC | | A | (M)* | | | M | |
| | Mode2 | SubModeA | | | | (M)* | | M | M |
| | | SubModeB | | | | A | (M)* | | |
| | Mode3 | SubModeA | | | | | M | (M)* | |
| | | SubModeB | | | | | | A | (M)* |

*The existence of self-transitions (re-entry into current mode) is a project specific decision. They could be used e.g. to reset timers or states (of controllers, filters, etc.).

The *Nominal AOCS Design* is assumed to be robust against expected parameter uncertainties (e.g. spacecraft CoM offset, unit misalignment, sensor noise), expected environmental disturbances (e.g. air-drag at solar minimum, orbit drift) and expected sensor outages (e.g. star tracker blinding, GNSS outages) leading to different measurement configurations (see Section 2.2.2).

The AOCS Safe Mode (sometimes even several safe modes) of a spacecraft is considered to be part of the *Nominal AOCS Design.* De facto every higher spacecraft has an AOCS safe mode, especially because this mode is often used almost unchanged for initial attitude acquisition after separation from launcher. The major task of a typical AOCS safe mode is to control the attitude and AOCS related mechanisms of the spacecraft such that:

- sufficient power can be generated by the solar arrays (attitude, SADM)
- communication with ground (possibly via relay satellite or mothership) is possible (attitude, steerable antenna)
  - establish a reliable command uplink (if command link is not continuously possible, at least the visibility pattern shall be unambiguously predictable)
  - provide sufficient telemetry to ground (allowing to define a safe recovery strategy)
- thermal conditions are kept within acceptable ranges (attitude)
- low power and propellant (consumables) consumption
- damage and contamination of payload and platform is avoided (e.g. instrument blinding, thruster plume impingement on rotational solar array, contamination of optical instruments by propellant plume, etc.).

The envelope of acceptable initial conditions of a safe mode (e.g. the maximum spacecraft rate or angular momentum at safe mode entry) is relevant for the parameterization of the FDIR in terms of monitoring limits (e.g. the spacecraft rate at which a transition to safe mode is triggered) and time to recovery (e.g. reconfiguration of RCS in case of a thruster stuck-open failure). The existence of an AOCS safe mode is often required by the costumer (e.g. by explicit requirements like “seven days survival in safe mode without ground contact”) and has proven useful to account for potential failures also in non-AOCS subsystems (thermal “too hot”, power “not enough”) and unexpected problems in general.

The general design goals of an AOCS safe mode are therefore:

- simple and reliable with respect to
  - used algorithms
  - used AOCS equipment
- clear definition of entry conditions of dynamics and s/c configuration (solar array, antennae, payload/instruments, etc.)
- robust with respect to:
  - used AOCS equipment
  - variable environmental conditions
- low in power consumption
  - to account for potential problems in power subsystem
- working in wide temperature range
  - to account for potential problems in thermal control subsystem

The obtained solutions are often based on sun or earth pointing attitude control with simple control algorithms using robust actuators (RCS, MTQ). It is however to be noted that a strong desire exists on customer’s side to use actuators in safe mode which do not alter the satellite’s orbit, i.e. reaction wheels and magnetorquers, if possible, and leaving the RCS as the last option. A gradual fallback approach in the failure recovery logic of the System FDIR can take this desire into account by using the RCS as the very last option (provided e.g. MTQ cannot be used). It is recommended that such customer desire is clearly formalized by the requirements baseline as the verification effort increases with more gradual fallback recovery logic.

For complex missions (like e.g. interplanetary science) it might be required to implement multiple safe modes with different concepts. In such cases the different safe modes are sometimes differentiated into “survival mode(s)” and “safe mode(s)”. Survival modes are characterized by less required resources compared to safe modes. Such resources could e.g. be calibration or context information (general availability or amount of), ground reaction time, favorable environmental conditions, or amount/complexity of required AOCS equipment.

## 2.2 Nominal Equipment Set

The *Nominal Equipment Set (NES)* comprises the whole set of AOCS equipment required to fulfil the objectives of the mission in the absence of faults. This set is assumed to be minimal in

the sense that it contains no single element which could be left out without violating any functional and/or performance requirement; i.e. it is not tolerant against any failure. The nominal equipment sets for individual AOCS main modes are subsets of the overall Nominal Equipment Set (see Figure 2-1 and Table 2-2).

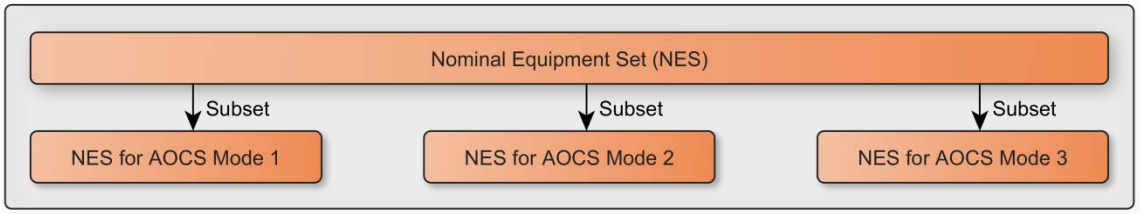


Figure 2-1 The nominal equipment sets for all AOCS modes are subsets of the overall NES.

In preparation for the following extension of the nominal equipment set described in Section 4.2 two things have to be decided: the desired granularity of the equipment modelling (see Section 2.2.1) and the considered measurement configurations of all AOCS modes (see Section 2.2.2).

Table 2-2: Exemplary NES for different AOCS modes and overall NES.

| AOCS Mode | Equipment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | GPS | STR | RMU | CESS | MAG | DSS | RW | MTQ | RCS | SADM |
| NES for Mode 1 | | | 1 | 1 | 1 | 1 | | 1 | 1 | 1 |
| NES for Mode 2 | 1 | 1 | | | | | 1 | 1 | | 1 |
| NES for Mode 3 | 1 | 1 | | | | | 1 | 1 | 1 | 1 |
| Overall NES | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

### 2.2.1 Granularity of Equipment Modelling

The granularity of the equipment modelling depends on the desired granularity of the possible redundancy configurations. If e.g. a 3-axes rate measurement unit (or similar a 3-axes magnetometer) is modelled as single item, it implies that this sensor can only be replaced in whole in case it fails. If it is on the contrary desired (and technically possible) to replace a single measurement axis of such a 3-axes unit by a single axis of another one, then all single axes should be modelled right from the start in the Nominal AOCS Equipment Set. This decision has to be made for each type of equipment individually and is required for all sensor/actuators which measure/act along different directions independently. Nevertheless, one should not forget that even if there are several independent measurement or actuation channels (which could in principle be substituted separately) these channels might be connected to the same front end electronic, power supply, or communication terminal, which affects all channels in case of its failure.

Figure 2-2 shows an exemplary nominal equipment set (NES) for an Earth observation satellite in low Earth orbit, in which the reaction wheels and magnetorquers have been modelled individually and the 3-axes rate measurement unit and the magnetometer as single items. The various NESs for the individual AOCS modes are illustrated below.

Remark: the granularity of the equipment modelling is a very important aspect when using the GAFE Structural Analysis, see [RD-1].

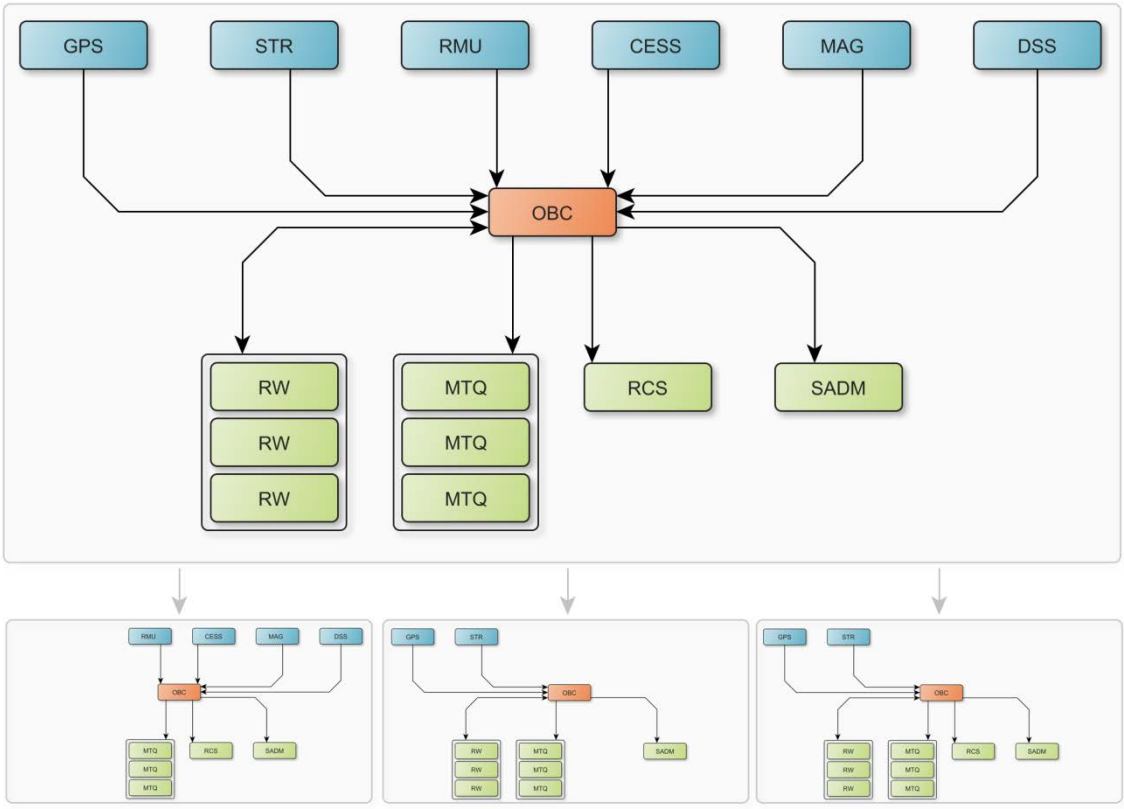


Figure 2-2 Exemplary nominal equipment set for a LEO satellite (top) and individual nominal equipment sets for different AOCS main modes (bottom).

### 2.2.2 Measurement Configurations

As mentioned above, the nominal AOCS design is assumed to be robust against expected sensor outages (temporary unavailability is no fault, but a normal operational constraint) like e.g. star tracker blinding, GNSS outages or Sun/Earth out of field of view of Sun/Earth sensor. For the detectability and isolability analysis of equipment failures during the extension of the NES in Section 4.2 it is necessary to define measurement configurations (as caused by expected sensor outages) the FDIR shall be able to cope with. These measurement configurations are nothing else than subsets of the NES (see Figure 2-3 and Table 2-4) of the different AOCS modes, in which one or several units are considered to be not available for a certain time (see Figure 2-3).

Which units or combinations of units are expected to be temporarily unavailable in a certain AOCS mode is defined by so-called unit unavailability vectors (UUV). For each AOCS mode there can be between zero and several UUVs.

Table 2-4 gives an example: The NES of AOCS mode 1 consists of four sensors: 1 RMU, 1 CESS, 1 MAG and 1 DSS. The considered measurement configuration for the FDIR design in this mode is defined by UUV 1, which says that there is a chance that during nominal operation up to 1 CESS and 1 DSS might be temporarily and potentially simultaneously unavailable. The UUV 1 in this example covers therefore four potential cases:

- 1x CESS and 1x DSS available, or
- 1x CESS and 0x DSS available, or
- 0x CESS and 1x DSS available, or
- 0x CESS and 0x DSS available.

In case two sensors could become potentially unavailable, but not simultaneously, one must define two UUVs, as e.g. done for the GPS and STR in AOCS mode 2. The potential cases there are simply:

- 1x GPS and 1x STR available, or
- 1x GPS and 0x STR available, or
- 0x GPS and 1x STR available.

In order to improve the traceability of the fault management design the entries in UUVs should be properly related to the possible reasons for sensor and/or actuator outages. A star-tracker could e.g. become temporarily unavailable because of the Moon in its field of view or because of overheating at a certain attitude maneuver. If there are two star-trackers with their lines of sight sufficiently separated, the outage reason Moon will affect only one of them at a time. Overheating on the other hand could also affect both units at the same time in case they mounted on the same side of the spacecraft. Similar correlations can also exist between units of different type, e.g. magnetometers and magnetorquers could become both functionally unavailable at the apogee of a highly eccentric orbit because of the weak magnetic field (see example in Table 2-3).

Such kind of unit unavailability need also to be explicitly considered during the extension of the equipment set for FDIR purposes. Independent of how many sun sensors one adds they all become unavailable during eclipse.

Table 2-3: Exemplary mapping between outage reasons and units.

| Outage Reason | STR1 | STR2 | STR3 | MAG1 | MAG2 | CAM1 | CAM2 | MTQ1 | MTQ2 | MTQ3 | … |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Moon in FoV Normal Mode | x | x | x | | | | | | | | … |
| Overheating during Maneuver | x | x | | | | x | | | | | … |
| Orbit apogee | | | | x | x | | | x | x | x | … |
| Solar flare | | | | | | x | x | | | | … |
| Eclipse | … | … | … | … | … | … | … | … | … | … | … |

During the extension of the NES in Section 4.2 the resulting extended equipment set must allow to fulfil the required detectability and isolability properties for all UUVs.

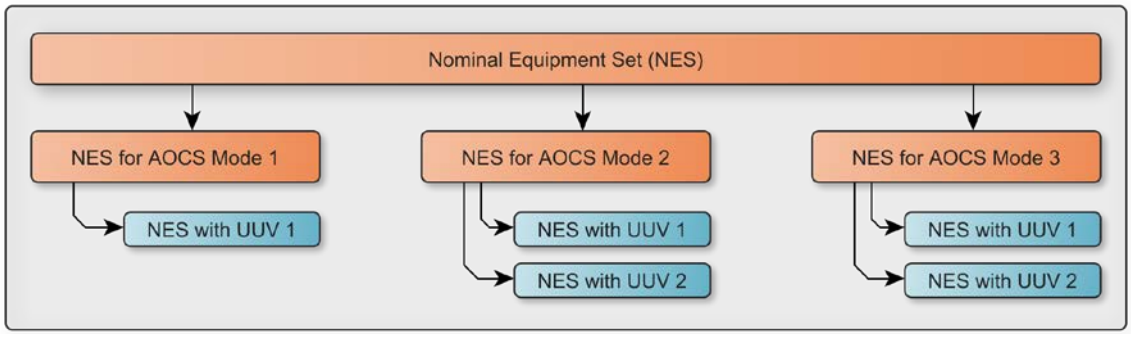


Figure 2-3 Exemplary nominal equipment sets of different AOCS modes and associated measurement configurations (expressed as NES and UUV).

Table 2-4: Exemplary list of unit unavailability vectors (UUV) per AOCS modes.

| AOCS Mode/ Meas.Config. | Equipment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | GPS | STR | RMU | CESS | MAG | DSS | RW | MTQ | RCS | SADM |
| NES for Mode 1 | | | 1 | 1 | 1 | 1 | | 1 | 1 | 1 |
| UUV 1 | | | 0 | 1 | 0 | 1 | | 0 | 0 | 0 |
| NES for Mode 2 | 1 | 1 | | | | | 1 | 1 | | 1 |
| UUV 1 | 0 | 1 | | | | | 0 | 0 | | 0 |
| UUV 2 | 1 | 0 | | | | | 0 | 0 | | 0 |
| NES for Mode 3 | 1 | 1 | | | | | 1 | 1 | 1 | 1 |
| UUV 1 | 0 | 1 | | | | | 0 | 0 | 0 | 0 |
| UUV 2 | 1 | 0 | | | | | 0 | 0 | 0 | 0 |

# 3 High Level Flow of FDIR Methodology

*This section presents the high level flow of the methodology for the AOCS FDIR design and development process of a spacecraft. It is assumed that all items of the Nominal AOCS Design as described in Section 2.1 are available at this point.*

## 3.1 Linear Representation

The FDIR methodology can be coarsely subdivided in seven 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. Tasks 1 to 3 comprise the complete FDIR design and are in principle independent of specific software tools (nevertheless, tools are quite useful here), tasks 4 to 7 cover the early verification and validation; these tasks are very specific in the sense that the approach there depends a lot on the tool(s) used.

A more detailed representation of the flow, which also distinguishes between inputs, tasks, intermediate results and decisions, is given in Figure 3-2 and Figure 3-3. In contrast to the linear representation the detailed one also shows the path back to re-entry points in case iterations are required.

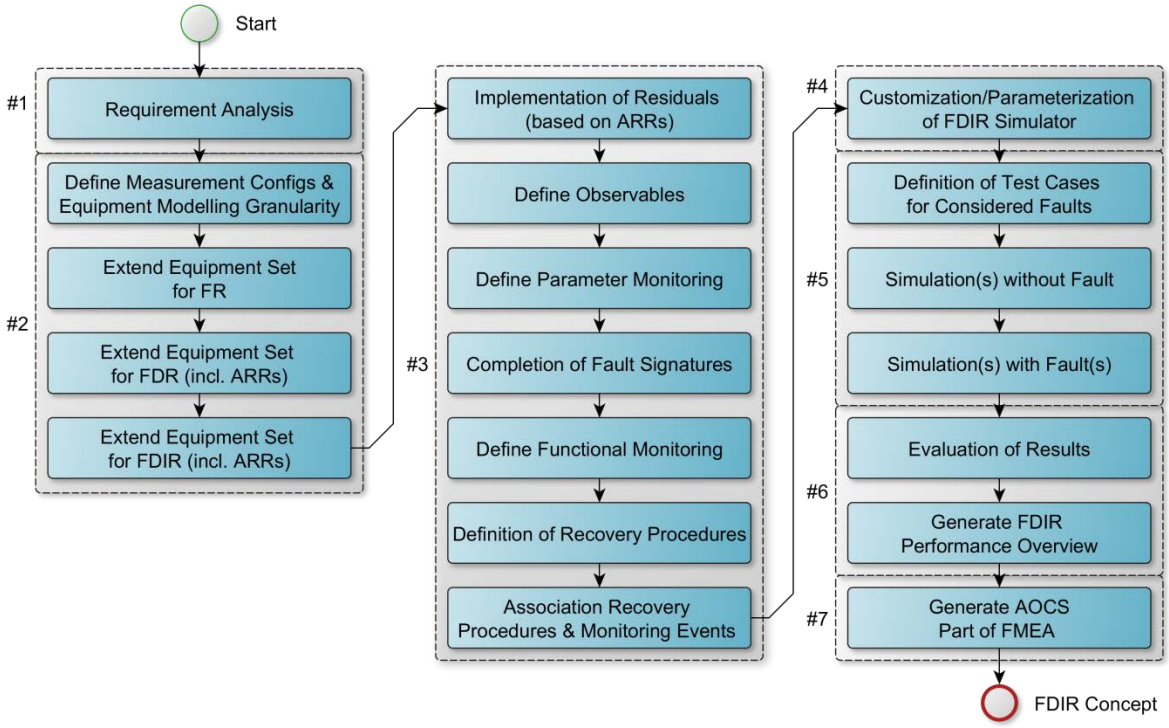


Figure 3-1 High level flow of FDIR methodology for spacecraft AOCS. Hash numbers indicate the corresponding tasks (e.g. #1 for task 1).

## 3.2 Detailed Representation

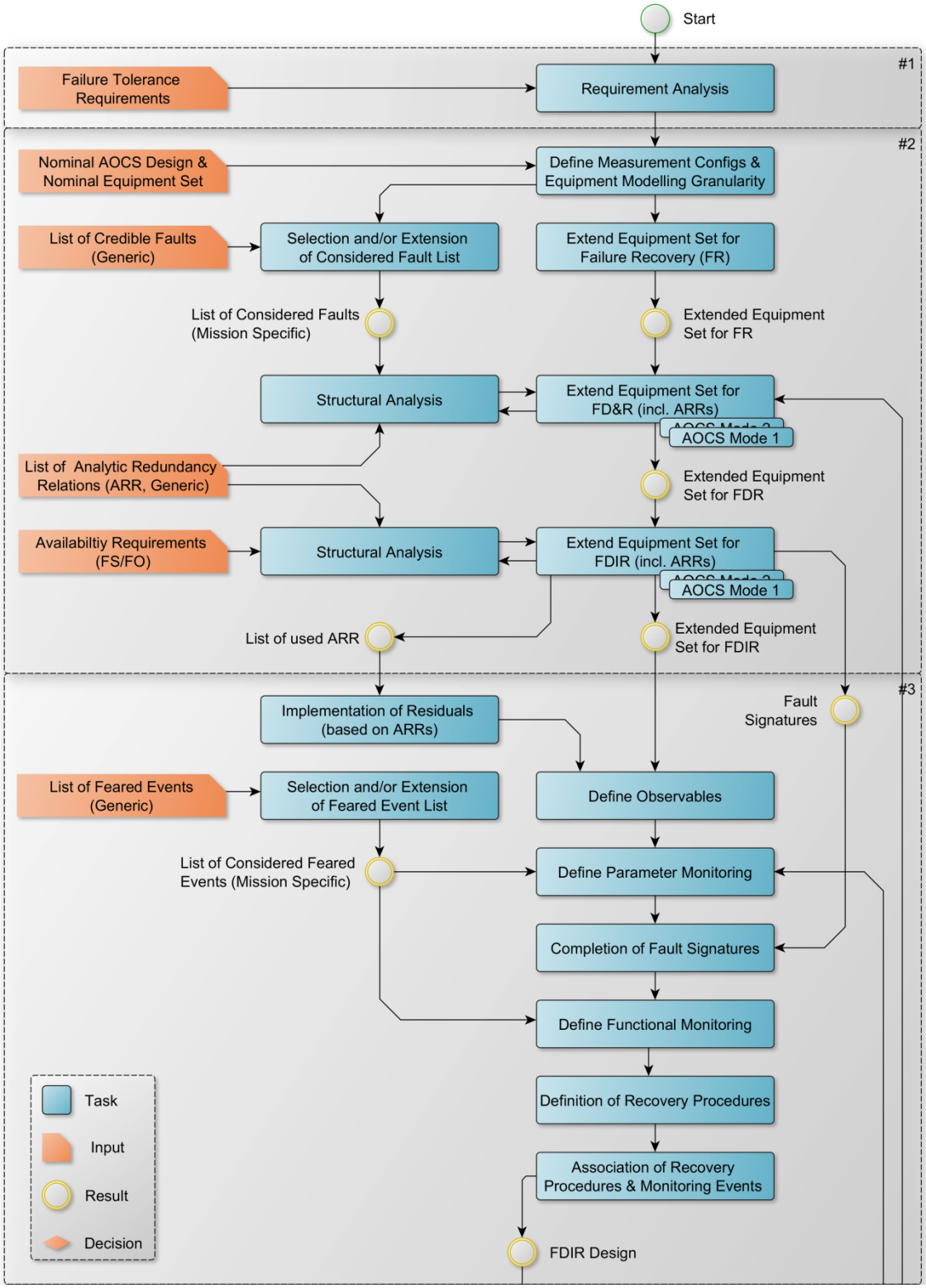


Figure 3-2 Detailed high level flow of FDIR methodology, part 1/2.

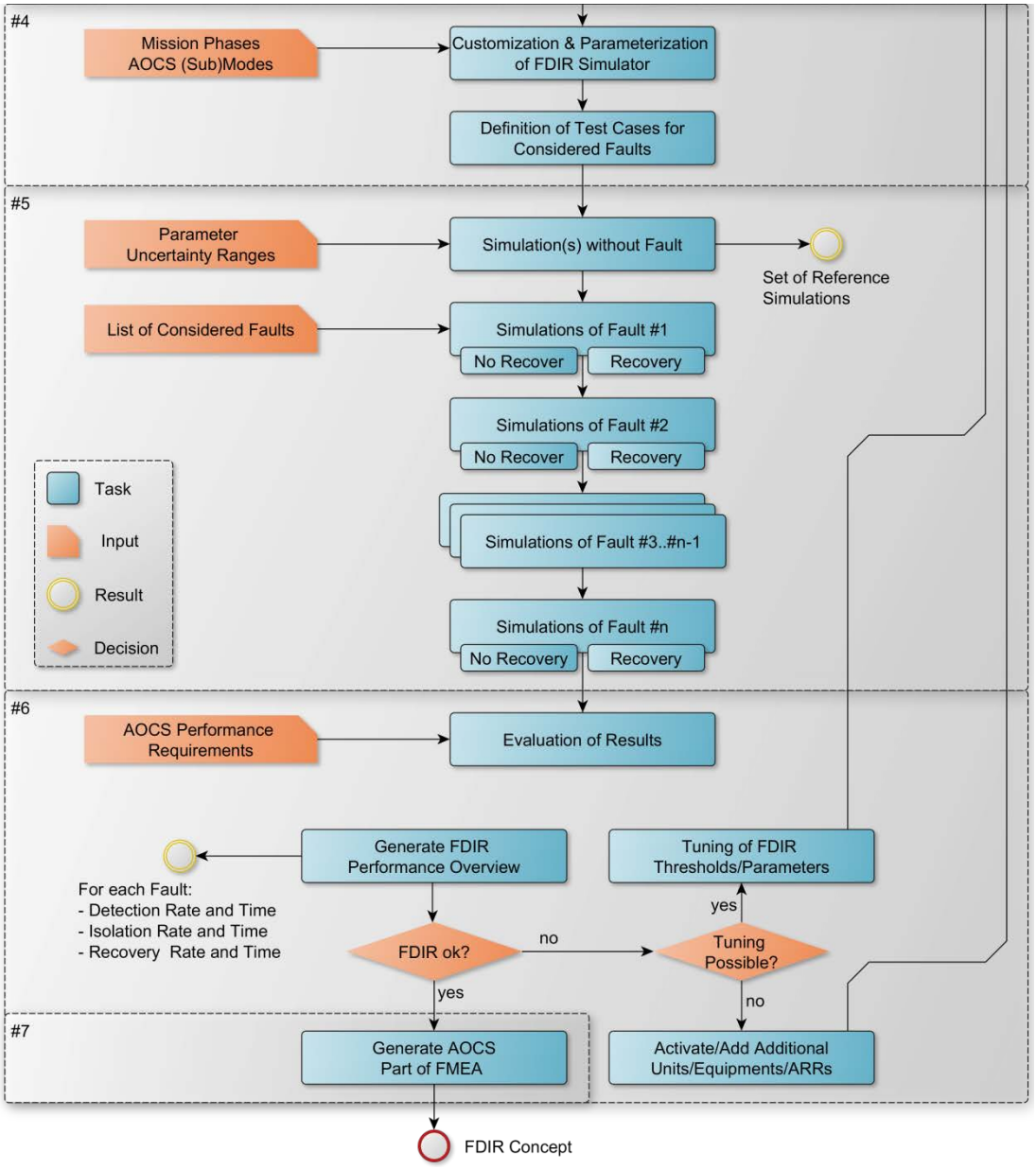


Figure 3-3 Detailed high level flow of FDIR methodology, part 2/2.

# 4 FDIR Methodology Tasks

*This section provides detailed descriptions of the different tasks to be carried out during the FDIR design and development process.*

## 4.1 Analysis of Fault Management Requirements (Task 1)

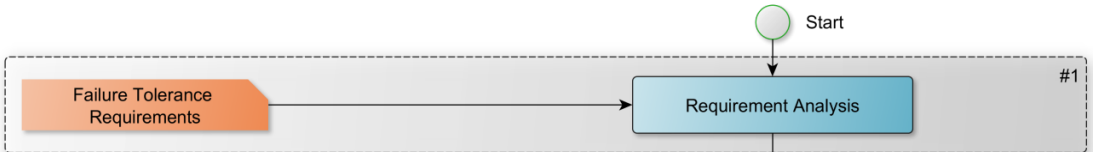


Figure 4-1 Elements of Task 1 (excerpt of high level flow).

The careful analysis of the fault management (FM) requirements of a space mission, documented in the Mission Requirements Document of the customer, is the first important step towards a concise, made-to-measure and robust FDIR concept. Although the specific FM requirements differ from mission to mission, most of them belong to one of the following categories:

- 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)

The sections ahead give more detailed information about the first three types of requirement categories with special focus on AOOCS. The topic reliability is not covered explicitly, because in early mission phases (the focus of this methodology) the specific units are normally not yet selected. Therefore the computation of the overall system reliability could only be performed based on rough estimates (e.g. differentiated by equipment type), which is not sufficient.

### 4.1.1 Failure Tolerance Requirements

Usually, the failure tolerance requirements are part of the customer specification of a space mission. They define the number and type of failures the system to be developed must be able to cope with. They are often linked to consequences which have to be avoided in case the failure happens. They are usually expressed similar to:

- *Single Failure Tolerance: Each satellite shall be able to sustain a single failure or operator error without critical or catastrophic consequences.*

Often these requirements include the concept of credible failures, i.e. the specified failure tolerance level is required against all *credible failures* (in components, parts, functions, and operators). These requirements are accompanied by the request to define a list of *non-credible failures*, which needs to be approved by the customer. Typical non-credible failures are:



Doc.No.: GAFE-UM-D7.5a
Issue: 2.0
Date: 13.06.2018

- Rupture of tanks (pressure and propellant)
- Damage of primary and load carrying spacecraft structures
- Fracture or short circuit in primary power bus
- Failures of antenna or associated cabling
- Locking of RF switches at intermediate positions

The much more rigorous *Two Failure Tolerance* requirement is usually made applicable to space missions involving human safety and is restricted only to failures leading to catastrophic consequences. An exemplary formulation is:

- *Two Failure Tolerance:*
  - *no single failure or operator error shall have major or critical or catastrophic consequences,*
  - *no combination of either:*
    - *two failures, or*
    - *two operator errors, or*
    - *one failure and one operator error,*

    *shall have catastrophic consequences.*

Very important in this context are the requirements making assumption on the simultaneity of failures, e.g.:

- *Two independent failures occurring simultaneously are considered as not credible.*

The impact of failure tolerance requirements on the system in general, but in particular on the AOCS subsystem and its FDIR design is huge; already a single failure tolerance requires at least one additional unit of each sensor and actuator. The procedure to extend the AOCS equipment set in order to make it compliant to the required failure tolerance is described in detail in Section 4.2.

Note: The fault management methodology presented in this document focuses on the most common top-level FM requirement, the single failure tolerance.

### 4.1.2 Availability Requirements

The failure tolerance requirements described in the section above define against how many and what type of failures the spacecraft must be able to cope with. What is not defined there is the concept to overcome occurring failures.

For space missions there are two main concepts describing how to handle failures, *Fail-Safe (FS)* and *Fail-Operational (FO)*. Their descriptions are given in Table 4-1 below.

Table 4-1: Definition of Fail-Safe and Fail-Operational.

| Concept | Description |
|---|---|
| Fail-Safe (FS) | A failure is autonomously detected and resolved onboard such that the scheduled operation of the concerned functionality is terminated and the affected subsystem, payload or spacecraft is switched into a safe state/mode (i.e. one in which the major functions are preserved) until ground intervenes to restore scheduled operations. Fail-Safe is the opposite concept to *Fail-Operational*.<br>Fail-Safe FDIR concepts support Survivability mission requirements. |
| Fail-Operational (FO) | A failure is autonomously detected and resolved onboard such that the scheduled operation of the concerned functionality is continued without the need for ground intervention. Fail-Operational is the opposite concept to *Fail Safe*.<br>Fail-Operational FDIR concepts support Availability mission requirements. |

Usually, not one single concept is used for the overall mission, but the concept to be used is defined for individual mission phases and/or AOCS modes. Normally, a fail-safe concept is used as default and fail-operational situations are either requested by direct or indirect requirements:

- Direct requirements, i.e. through explicit definition of fail-operational mission phases. E.g. if a continuous operational state is required to achieve a mission objective (typical example are delta-V manoeuvres) and which otherwise leads to severe mission operational implications or even mission loss.
- Indirect requirements, i.e. through requirements on the availability of the spacecraft (e.g. to deliver/acquire desired payload products).

Examples for direct requirements are:

- *For clearly identified critical mission phases (e.g. Orbit insertion) fail-operational shall be implemented.*
- *The FDIR shall provide automatic recovery from all credible anticipated failures which do not require ground decision.*

Indirect requirements (via availability) are e.g.:

- *The Satellite shall be design to provide in-orbit availability for the Payload Mission data greater than XX over the satellite nominal life time, after acquisition of the operational orbit and commissioning, and taking into account the effects of space environment, but excluding the case of mission loss.*
- *The constellation shall be designed to provide an operational availability during the operational phase of XX months of higher than XX.*
- *The satellites shall be designed to support payload operations for a minimum of XX YY-day science cycles before the end of the science mission with greater than ZZ% continuity within that cycle.*

In general the use a fail-operational concept for the AOCS demands a much higher degree of autonomy compared to a fail-safe concept. This comes along with a much higher FDIR design and validation & verification effort, because for fail-operational situations:

- every credible fault has to be anticipated in the design,
- detection of all lower level failures need to be possible before they lead to failure of the AOCS itself (see Section 4.2.2)
- isolability of all faults has to be ensured (see Section 4.2.3),
- purposeful recovery actions need to be made available for every credible fault (see Section 4.3.6)

The result of the availability analysis is a breakdown of the mission (expressed in terms of e.g. mission phases, AOCS modes, spacecraft configurations, or combinations of these) into precisely defined situations, in which either a FS or FO FDIR concept shall be implemented (see example in Table 4-2).

For the AOCS a fail-safe concept results in the necessity of being able to detect all credible faults. A fail-operational concept requires in addition that all credible faults can be detected and isolated (unambiguously identified), which required much more effort in terms of analysis and finally hardware and/or analytical FDI models.

Table 4-2: Exemplary availability concept per mission phases and AOCS modes.

| Mission Phase | AOCS Mode | Fail-Safe | Fail-Operational |
|---|---|---|---|
| Mission Phase A | | | |
| Phase A | AOCS Mode 1 | x | |
| | AOCS Mode 2 | x | |
| Mission Phase B | | | |
| Phase B | AOCS Mode 1 | x | |
| | AOCS Mode 2 | | x |
| | AOCS Mode 3 | | x |
| | AOCS Mode 4 | x | |
| Mission Phase C | | | |
| Phase C | AOCS Mode 1 | | x |
| | AOCS Mode 2 | | x |
| | AOCS Mode 3 | | x |

### 4.1.3 Best-Practice Requirements

The relation to AOCS FDIR in mind, the following lists of requirements have been collected from space missions reviews, providing generic requirements in different categories intended to make the overall FM design and FDIR implementation transparent, reliable and flexible. Since the mission reviews performed in the first phase of the GAFE study revealed significant differences in the amount and level of detail of FM related requirements (e.g. depending on costumer, project team, etc.), the idea behind this collection is to cross-check the given (costumer) and derived (system/subsystem level) requirements with the ones collected in order to complement them if needed.

Requirements which are directly applicable in this methodology are listed in the corresponding section below. Others, like e.g. FDIR-BP-102 (Spare capacity (25% at launch time) for additional monitoring and recovery actions shall be available…) apply to the overall system and cannot be covered or verified by AOCS alone. Such requirements are listed only here.

Table 4-3: List of best-practice FM requirements regarding general FDIR.

| Req. ID | Fault Detection, Isolation and Recovery |
|---|---|
| FDIR-BP-101 | FDIR shall not trigger on one sample of a parameter. Possibly redundant readings shall be verified. As a minimum, contiguous samples shall be used. |
| FDIR-BP-102 | Spare capacity (25% at launch time) for additional monitoring and recovery actions shall be available in all tables and memory areas needed for monitoring and recovery actions. |
| FDIR-BP-103 | HK Telemetry shall be continuously generated and recorded in all modes of operations, including safe mode. |
| FDIR-BP-104 | Failure detection and management functions shall avoid continuous production of the same anomaly report packet if the same failure is detected with a specified number of monitoring cycles. |
| FDIR-BP-105 | After launch without ground contacts in nominal and one-failure situations, the avionics shall support satellite survival, without subsequent loss of mission, for a duration of at least:<br>• XX orbits prior solar array deployment (if applicable)<br>• YY days after solar array deployment in LEOP<br>• ZZ days in COP and MOP |
| FDIR-BP-106 | All intelligent units and instruments shall perform regular self-checks, and shall report them.<br>Note: Intelligent units are those able to generate TM packets, and to process TC packets. |
| FDIR-BP-107 | The fault management functions at all levels shall be able to carry out consistency verification checks on redundant sensor readings whenever redundancy is available, before starting the recovery actions. |
| FDIR-BP-108 | The spacecraft shall maintain a list of available, suspected and failed hardware units. This information shall be updatable by dedicated telecommand and available in telemetry. |

| | |
|---|---|
| FDIR-BP-109 | The management of anomalies (within a unit, subsystem or instrument) shall be handled in a hierarchical manner, such that resolution is sought on the lowest possible level. Failures that cannot be handled at a given level shall be handed over to the next higher operational instance, the highest one being the ground. |
| FDIR-BP-110 | Where possible, failure recovery actions shall first attempt a software reboot before considering a hardware reconfiguration of the affected units. |
| FDIR-BP-111 | The activation of a redundant unit or functional path shall not require a change of the configuration or operational status of another unit. |
| FDIR-BP-112 | If an on-board processor is switched from a main to a redundant unit (or vice versa), the switchover shall be such that operations can continue safely. Note: This implies that either the operational context need not be reloaded from ground, or the new processor can be loaded with a safe default context before the switchover. |
| FDIR-BP-113 | The fault management shall include monitoring of individual equipment measurements (e.g. time stamp updates, validity flags, measurement ranges) to detect corrupted or old data. |
| FDIR-BP-114 | Configuration and health status data shall be stored in safeguard memory. |

Table 4-4: List of best-practice FM requirements regarding command and control.

| Req. ID | Command, Control and Visibility |
|---|---|
| FDIR-BP-201 | During all mission phases there shall be no requirement for the ground to send telecommands in nominal or contingency cases with a response time of less than XX hours, including the round trip time of the signal. |
| FDIR-BP-202 | All parameters used for autonomous operations (e.g. thresholds for limit checking or thresholds and biases for attitude control), including fault management, orbit and attitude control, etc., shall be updatable by telecommand and available in telemetry. |
| FDIR-BP-203 | Anomalies and actions taken to recover from them shall be reported in event driven packets. |
| FDIR-BP-204 | It shall be possible to reconstruct from telemetry the conditions leading to the generation of an event. |
| FDIR-BP-205 | The on-board autonomy shall be able to access any non-science telemetry packet generated by any on-board user. This includes in particular non-periodic event packets which can be used to trigger recovery actions at system or sub-system level, as a result of an anomaly occurred (and detected) in another subsystem. |
| FDIR-BP-206 | For control of all FDIR surveillances (i.e. low-level parameter monitoring functions implemented in the individual on-board software packages for health monitoring at subsystem/unit level) dedicated telecommands shall be available as follows:<br>• enable/disable single surveillances.<br>• enable/disable recovery action of single surveillances.<br>• enable/ disable all surveillances.<br>• modify the surveillance definition (thresholds, filters). |

| | |
|---|---|
| FDIR-BP-207 | It shall be possible to request a report of all defined surveillances, giving the list of surveillances including their complete definition (surveillance ID, parameter being monitored, thresholds applied, filters applied). |

Table 4-5: List of best-practice FM requirements regarding system reconfiguration.

| Req. ID | System Reconfiguration |
|---|---|
| FDIR-BP-301 | The maximum duration of an on-board reconfiguration shall be deterministic. |
| FDIR-BP-302 | All on-board reconfigurations shall end with an unambiguously known and observable state of all involved elements (hardware and software). |
| FDIR-BP-303 | The capability shall be provided for ground to allocate which of the redundant units are included in the nominal chain and which in the redundant chain. Note: This enables redundancy to be restored without reconfiguring the on-board hardware, and also enables a failed unit to be removed from both the nominal and redundant chains while maintaining the rest of the redundancy of the chain. This new configuration will be applied after a processor restart. |
| FDIR-BP-304 | Redundancy switching at unit level shall not require changes in telecommands directed to the operational unit. Note: This allows previously loaded commands (e.g. mission timeline, OBCPs) to address the current operational unit. |

Table 4-6: List of best-practice FM requirements regarding safe mode.

| Req. ID | Safe Mode |
|---|---|
| FDIR-BP-401 | Entry into safe mode shall be the result of the crossing of clear spacecraft-level safety critical dead bands, or of a clear case in which the low-level FDIR recovery was not possible. |
| FDIR-BP-402 | It shall be possible to enable/disable autonomous entry, and to force entry into safe mode by telecommand. Autonomous entry shall be enabled by default. |
| FDIR-BP-403 | The transition to safe mode, once started, shall not be interruptible. |
| FDIR-BP-404 | Safe mode shall, in each mission phase, guarantee the achievement of an indefinitely stable safe condition from any possible initial condition caused by any single failure (however improbable) that triggers a safety monitor (e.g. worst case possible dynamic conditions, worst case timings). |
| FDIR-BP-405 | The safe mode final condition shall be defined such that: uninterrupted power supply, as required for spacecraft safety, is provided; a thermally safe attitude is maintained; communications with the ground are guaranteed. |
| FDIR-BP-406 | Recovery from safe mode shall be undertaken under ground control. |
| FDIR-BP-407 | The spacecraft state variables shall be properly reinitialised for execution of the safe mode, and no residual values coming from previous spacecraft modes shall endanger the safe mode execution or recovery to normal mode. |



Doc.No.: GAFE-UM-D7.5a
Issue: 2.0
Date: 13.06.2018

| | |
|---|---|
| FDIR-BP-408 | No residual values of spacecraft state variables after entry and execution of safe mode shall remain in the recovered normal mode. |

Table 4-7: List of best-practice FM requirements regarding testing.

| Req. ID | Testing |
|---|---|
| FDIR-BP-501 | It shall be possible to checkout/test all equipment on ground and in flight |
| FDIR-BP-502 | It shall be possible to activate any provided diagnostic mode of a non-operating unit without interfering with the nominal operation of the spacecraft. |
| FDIR-BP-503 | No fault management function shall trigger on test data generated by a unit operating in test mode. |
| FDIR-BP-504 | Entering a test mode shall not require (or imply) disabling of fault management functions. |
| FDIR-BP-505 | It shall be possible to inject simulated faults in order to stimulate all FDIR mechanisms (residual generation, monitors) on purpose. This can either be done on hardware level (AOCS units, EGSE, MGSE, OGSE) or on software level (e.g. in the sensor processing). |

### 4.1.4 Optimization Criteria

Besides the different requirement classes discussed above there are also other constraints or optimization criteria to consider during the design and development of the FDIR. Such aspects are e.g.:

- Mass
  - direct: for redundant equipment
  - indirect: for additionally required solar array area, radiator area, etc.
- Cost
  - direct: for redundant equipment
  - indirect: for additionally required effort for design (e.g. for algorithms), validation, verification, etc.
- Power consumption (for redundant equipment)
- Reliability
- Computational load: e.g. caused by
  - sensor processing algorithms of hot redundant units
  - evaluation of analytic redundancy relations (ARR)
  - parameter and functional monitoring functions of FDIR
- Schedule
- Verification & validation effort
- Speed/Duration of

- Fault detection
- Fault recovery

The weighting of importance of such constraints or optimization criteria is usually quite mission specific and requires careful trade-off on system level. If the mass of the spacecraft (without redundancy) is e.g. already quite close to the maximum launcher capacity, emphasis will lie on an FDIR solution with small additional mass. If the performance of the foreseen OBC is low, high fidelity model-based FDI might be penalized.

Remark: the GAFE Structural Analysis (see [RD-1]) allows as weighting of the cost items “mass”, “cost (monetary)”, “power consumption”, and “computational load”.

## 4.2 Extension of Nominal Equipment Set (Task 2)

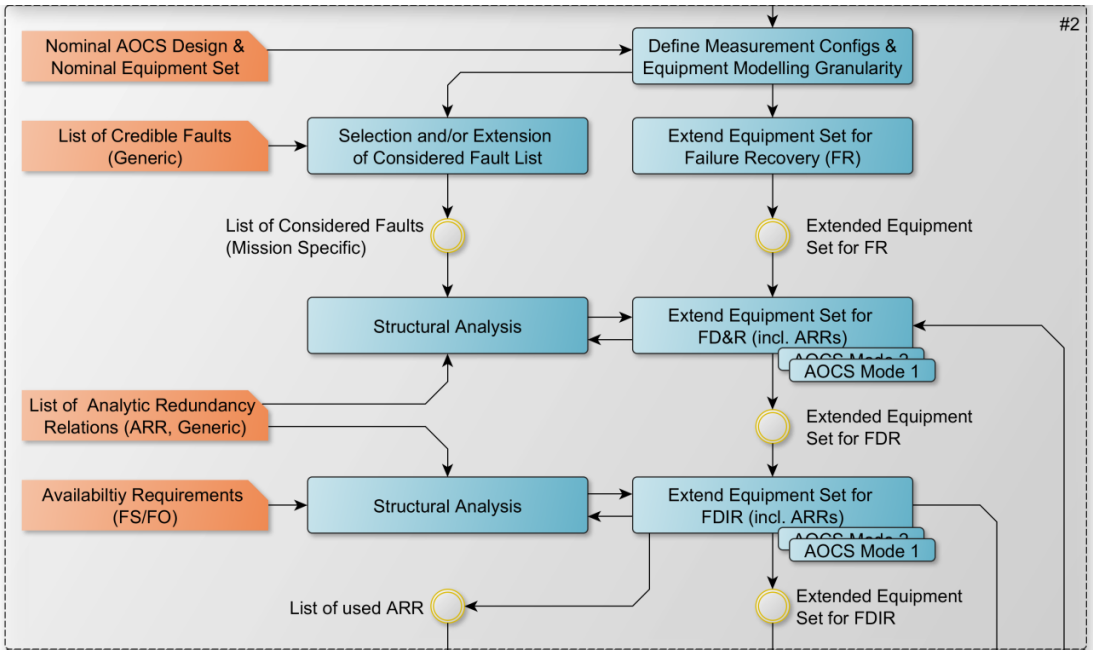


Figure 4-2 Elements of Task 2 (excerpt of high level flow).

This section deals with the extension of the nominal equipment set in three steps, each of them adding additional abilities to the set. These are:

1. Extend the set such that it becomes compliant to the failure tolerance requirement in terms of recovery: if a unit fails, there has to be an adequate replacement for it.
2. Extend the set such that it becomes compliant to the failure tolerance requirement in terms of failure detection: guarantee that if a failure in any unit occurs, it can be detected.
3. Extend the set such that it becomes compliant to the availability requirements: in which situations (e.g. mission phases, AOCS modes) the AOCS has to stay operational in case of a failure (fail-operational) in contrast to the case that a transition to a safe mode is acceptable (fail-safe). Fail-operational situations demand additional capabilities in terms of failure isolation (guarantee that if a failure in a unit occurs, it can be unambiguously identified).

In general these three extensions consist of activating or adding additional units, equipment and/or algorithmic features. The approach described hereafter focusses on “single failure tolerance”. Double failure tolerance, usually only requested for manned space missions, is not covered.

### 4.2.1 Extended Equipment Set for Failure Recovery (Step 1)

The goal of this step is to extend the nominal equipment set such that it becomes possible to replace any failed unit (once its failure has been isolated) with a redundant one by reconfiguration of the system.

Exceptions are units, which are so reliable that their failure is considered not credible (such units would be members of the non-credible failure list agreed between contractor and costumer). For the perimeter of the AOCS this classification applies e.g. often to propellant and pressure tanks of reaction control systems.

The proposed procedure for this extension step consists of two tasks:

- Task 1: duplicate all units of the nominal equipment set (see Figure 4-3).
- Task 2: investigate equipment by equipment for geometrical and/or functional intra-equipment redundancies. If such redundancies exist, they should be exploited by removing unnecessary units and replacing and/or reorienting the remaining ones. Typical examples are to replace 2x3 reaction wheels by 1x4, or 2x2 star tracker by 1x3 (see Figure 4-4).

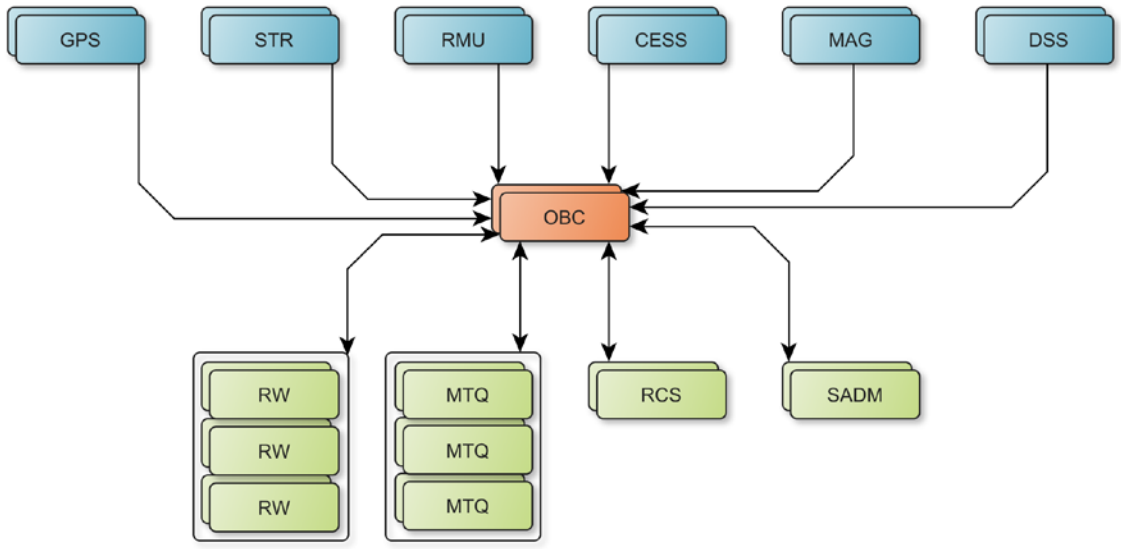


Figure 4-3 Extended AOCS Equipment Set after duplication of units (end of task 1).

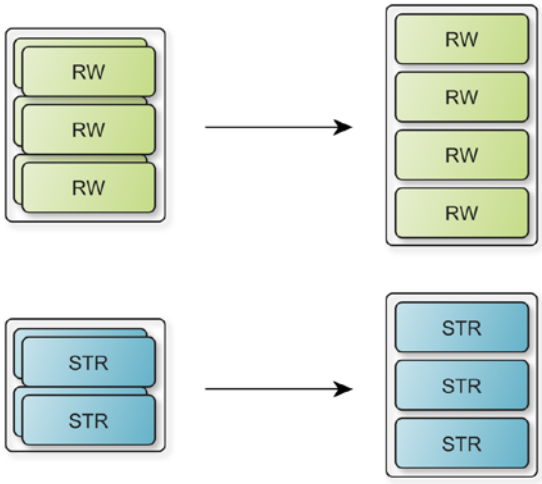


Figure 4-4 Examples in which geometrical redundancies can be exploited to remove units.

It is important that every modification needs to be properly investigated in order not to violate any functional or performance requirement of the nominal AOCS design, e.g. because of altered torque/momentum envelopes of the 1x4 reaction wheels after a single wheel failure or different blinding conditions of the rearranged star trackers.

For position sensitive units like e.g. thrusters or relative navigation sensors for proximity operations one needs to make sure that the finally chosen units can be accommodated (in position and orientation) compatible with the requirement of the nominal AOCS design (even in case of pure duplication).

At this point in time it is also meaningful to check if the equipment set contains equipment types, which are only available from the suppliers in certain configurations. Airbus's Coarse Earth Sun Censor (CESS) e.g. is only available with tripple redundancy. From this point of view it makes sense to consider this hardware related redundancy in the extended equipment set already now (see Figure 4-5).

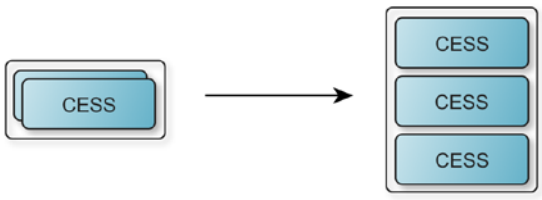


Figure 4-5 Example for redundancy concept, driven by COTS product constraints.

Besides the number of units and their accommodation on the spacecraft, it is also important how the units are electrically connected to OBC, RIU, PCDU, MilBus etc., i.e. in terms of power supply and TM/TC. If a unit would e.g. be only connected to one OBC or RIU (remote interface unit) side, a failure of this OBC/RIU side would additionally cause of loss of this unit through the required switch-over to the other side. Therefore it is desirable to perform cross-strapping (for power supply and communication) in order to increase the overall system reliability. If one unit

fails a redundant unit can take over without implying a complete switch-over to a redundant chain. On the other hand there is great benefit in functionally fully independent equipment chains (e.g. the standard nominal and redundant concept) because this reduces significantly the FDIR complexity and therefore verification effort. This task is a combined trade-off at system level with strong interaction among AOCS, electrical and FDIR engineering.

Anyhow, the result of the extension step is the Extended Equipment Set for Failure Recovery (EES-FR, see Figure 4-6) which allows that the functionality of any failed unit of the nominal equipment set can be sufficiently replaced by another one (e.g. one failed star tracker by another one) or the remaining ones (e.g. one failed reaction wheel by the remaining three).

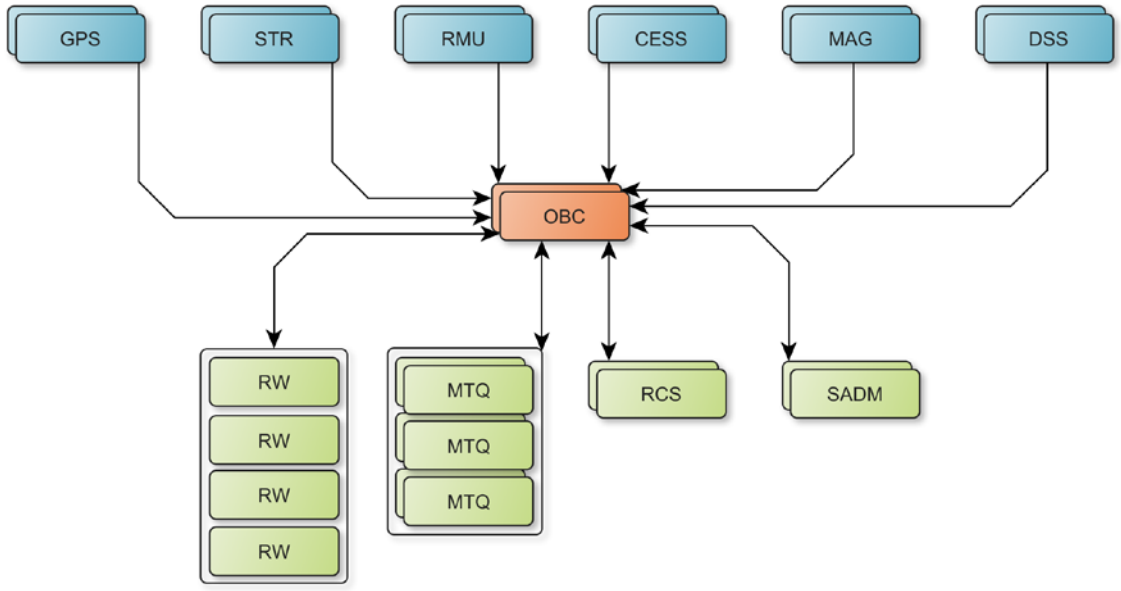


Figure 4-6 Exemplary Extended Equipment Set for Failure Recovery (EES-FR).

Note: Even if it often leads to the same result as the classical procedure “add one additional unit of each type”, the twofold approach described in this section has the advantage of forcing the FDIR designer to explicitly think about the consequences of removing any direct redundancy.

### 4.2.2 Extended Equipment Set for Failure Detection & Recovery (Step 2)

Unlike the first, the second extension step cannot be performed for the whole equipment set at once. It needs to be performed for each main AOCS mode separately, because the set of active units is usually different for each mode. The goal of step 2 is to modify the nominal equipment set of each mode such that a single failure in any unit can be at least detected. Its isolation (unambiguous identification), is not required here. Possible modifications to achieve full detectability of all considered failures are the following ones:

a) Foresee activation of units already existing in *Extended Equipment Set for Failure Recovery* that have not been used so far in the AOCS main mode under investigation.

b) Foresee use of analytic redundancy relations (ARR), i.e. algorithms using available system information (usually sensor measurements and actuator commands) by means

of mathematical and/or physical models to derive measures of consistency between different elements of the system.

c) Add additional units (hardware) to the *Extended Equipment Set for Failure Recovery* and foresee its additional activation in the investigated AOCS mode. The additional unit can either be of an already existing type, or it is the first one of an equipment type so far not used on the spacecraft.

These three modifications are further explained in the following subsections. A well suited analysis method for this step is the so-called Structural Analysis. An overview and introduction to this method is given in Section 5.

#### 4.2.2.1 Activation of Existing Units

The additional activation of already existing units for the purpose of improved failure detection is usually preferred approach as it implies the least impact. No additional hardware is required; the processing algorithms are already in place (from the nominal design); only the additional power and wear-out of the unit to be activated have to be considered.

Figure 4-7 shows a possible starting situation for this step. The AOCS main mode under investigation requires the nominal units displayed as solid blocks to be active. The other units of the extended equipment set for failure recovery (as derived in Section 4.2.1 and displayed as semi-transparent blocks) are nevertheless available and could be activated to improve the detectability of failures.

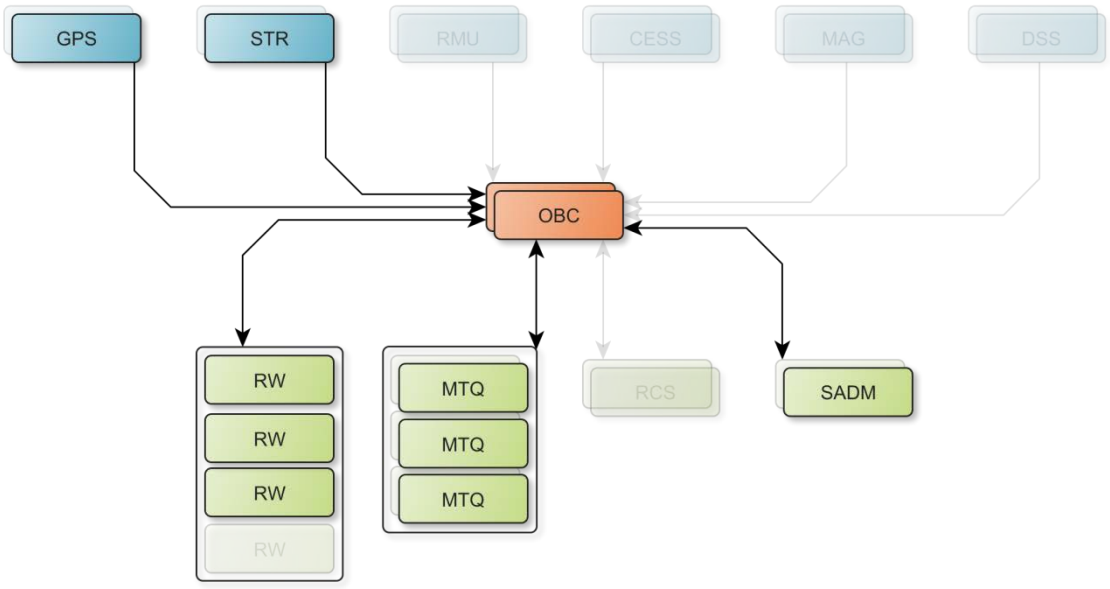


Figure 4-7 Nominal equipment set for main mode under investigation (solid units) and inactive units from extended equipment set for failure recovery (semi-transparent units).

If e.g. the measured attitude of the only active star tracker would slowly drift away, this failure could not be detected by means of the active units of the original configuration. One possible

solution to the problem would be to additionally activate the second (already available) star tracker (see Figure 4-8), which would allow a comparison of the two measured attitudes and thus the detectability of this kind of failure (in any of the two star trackers).

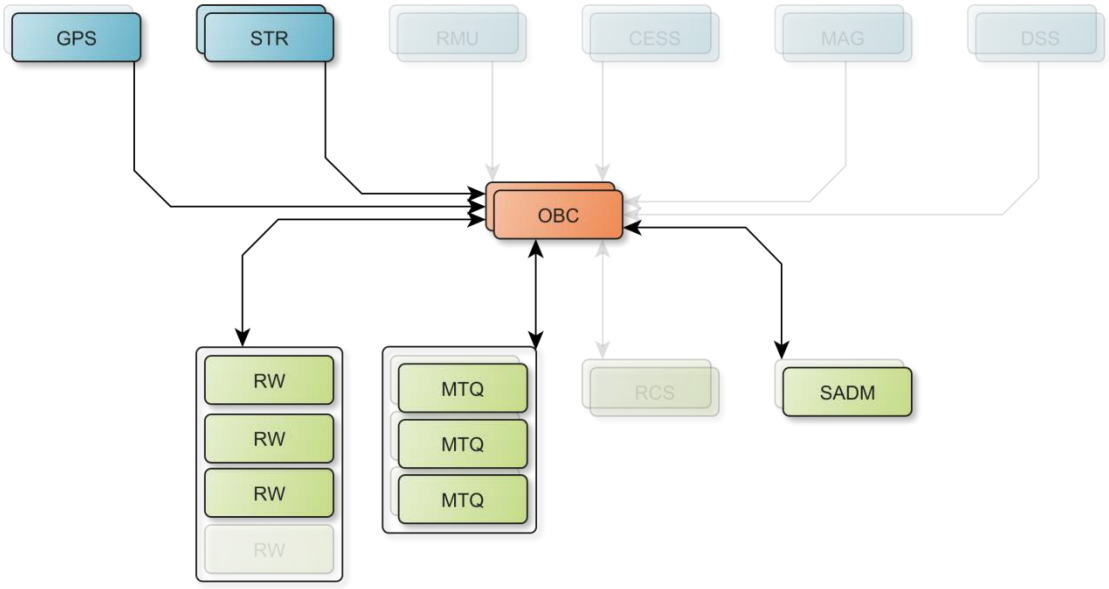


Figure 4-8 Additional activation of second star tracker to enable detectability of star tracker failures for both star trackers.

#### 4.2.2.2 Use of Analytic Redundancy Relations

In addition to the activation of available (but so far inactive) units there is the possibility to foresee the use of analytic redundancy relations (ARR), i.e. algorithms using available system information (usually sensor measurements and/or actuator commands) and mathematical and/or physical models to derive measures of consistency between different elements the system (see Figure 4-9). A simple example for this concept is illustrated in Figure 4-9, where the (available but inactive) rate measurement unit has been activated and a simple ARR was added. The ARR takes the derivative of the spacecraft attitude measured by the single STR to obtain an estimate of the spacecraft rate. This rate estimate can then be compared to the spacecraft rate measured by the RMU in order to detect failures in the STR measurement, the RMU measurement, or both.

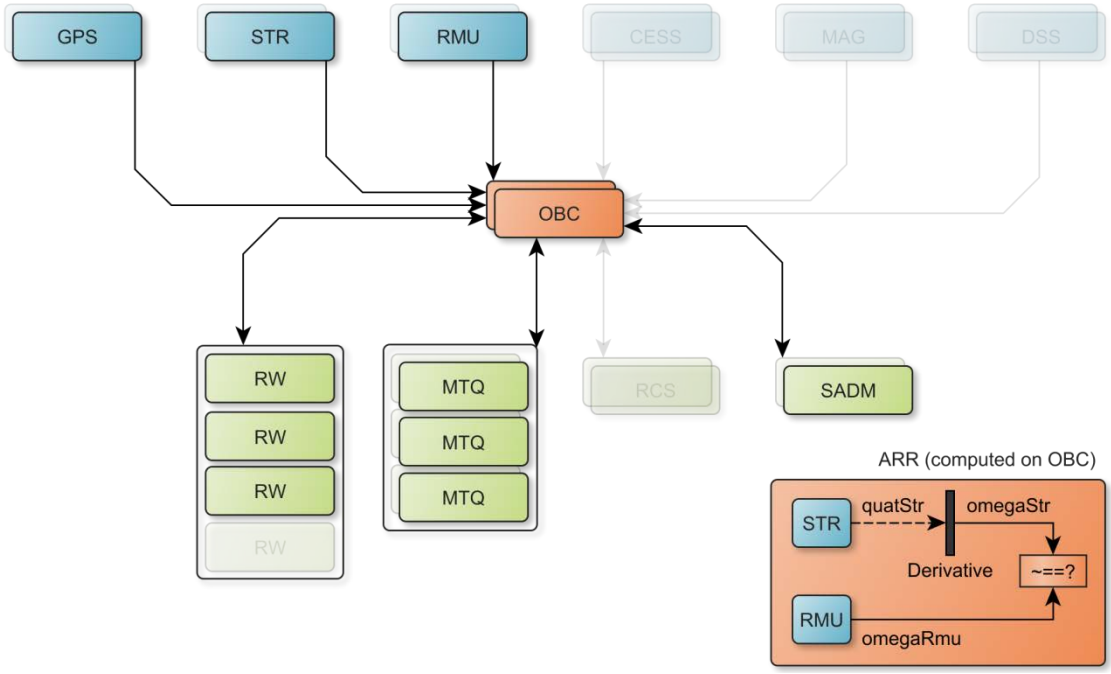


Figure 4-9 NES for main mode under investigation plus activated RMU from EES-FR and analytical redundancy relation (ARR) to compare spacecraft rate derived from STR attitude measurement with spacecraft rate measured by RMU.

#### 4.2.2.3 Additional Hardware

If the activation of additional units and/or the addition of ARR is not sufficient (or desired) to achieve detectability of certain failures, there is still the possibility to add additional hardware (units or completely new types of equipment) to the extended equipment set. This option is usually the last one to pick, because it is probably the most costly (in terms of money, mass, V&V effort, etc.).

#### 4.2.2.4 Summary of Step 2

When step 2 is finished, its result is the Extended Equipment Set for Failure Detection & Recovery (EES-FDR), which consists of the hardware configuration and the set of analytical redundancy relations to be used. The obtained EES-FDR allows to detect failures in all active units and to substitute any single failed unit (in the functional sense).

If the AOCS main mode under investigation requires only a Fail-Safe concept, the failure detection would be autonomously performed in the currently investigated mode, but the isolation of the failure and the reconfiguration of the system would happen after a mode transition to a safe mode based on ground based investigations and decisions. In this case step 3 can be skipped for this mode.

Even if full isolation of all anticipated failures is not possible with the EES-FDR, it often allows partial isolation, e.g. that the failure is either in the active STR or in the active RMU. This information is valuable for further investigation and should be reported to ground.

### 4.2.3 Extended Equipment Set for Failure Detection, Isolation & Recovery (Step 3)

Extension step 3 need to be executed only for main modes for which a fail-operational (FO) concept has to be implemented. Like the second step this one needs to be performed mode by mode, because the set of active units may be different in each of them. Also like in Step 2, the structural analysis (see Section 5 and [RD-1]) is well suited to support this step.

The goal of step 3 is to modify the EES-FDRs for FO modes to become EES-FDIRs, i.e. that any single failure in any unit must not only be detectable, but also isolable (unambiguously identifiable). The possible modifications to achieve full isolability are the same as for the detectability in step 2, i.e. the following ones:

a) Foresee activation of unit(s) already existing
b) Foresee use of analytic redundancy relation(s) (ARR)
c) Add additional unit(s)/equipment(s)

When step 3 is finished, its result is the Extended Equipment Set for Failure Detection, Isolation & Recovery (EES-FDIR), which consists of the hardware configuration and the set of analytical redundancy relations to be used. The obtained EES-FDIR allows to detect and isolate failures in all active units and to substitute any single failed unit without the need of a mode change (FO).

Remark: The system implications and trade-offs to be performed for a fail-operational (FO) concept are much more significant and go beyond the perimeter of the AOCS. It has to be recognized that fail-operational FDIR involves also the potential reconfiguration of the on-board computer. For this reason, it needs to be kept in mind that fail-operational FDIR concept is typically a system level activity with iterations over the overall system redundancy concept including the cross-strapping of the units between the redundant on-board computers or context-switching between the on-board computers

## 4.3 Definition & Implementation of FDIR Concept (Task 3)

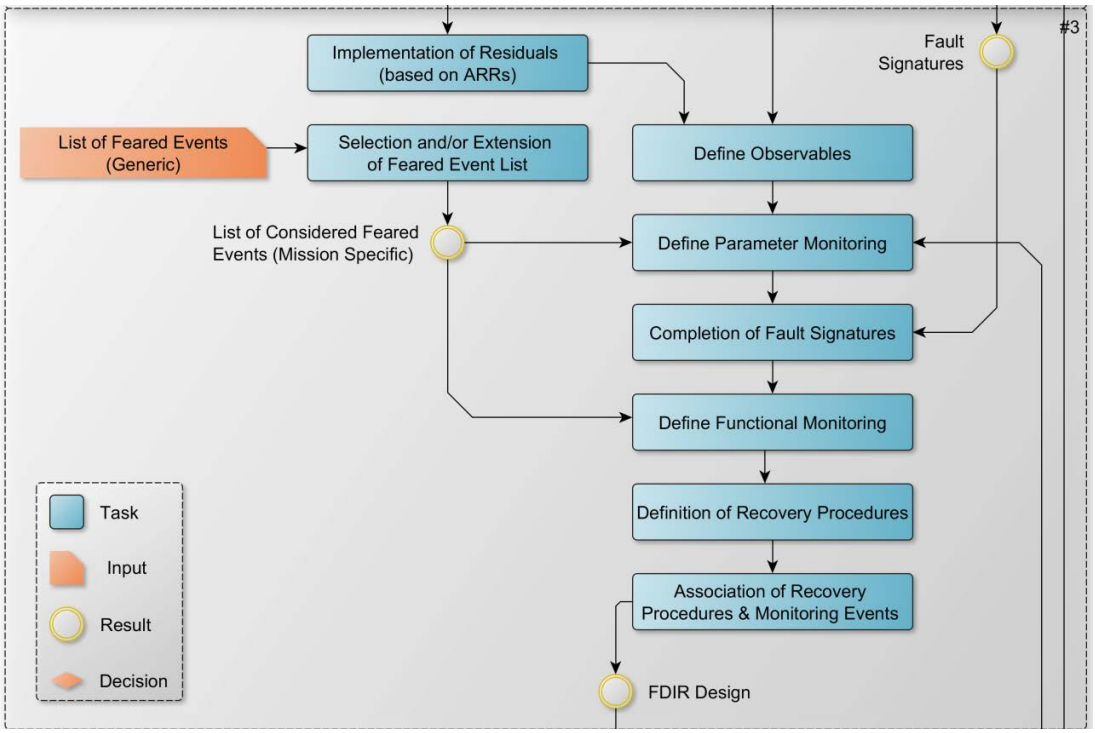


Figure 4-10 Elements of Task 3 (excerpt of high level flow).

This section covers the tasks related to the definition and implementation of the FDIR. The order of tasks is oriented on the typical information flow inside the FDIR (see Figure 4-11). First, required but so far unavailable variables (e.g. residuals from analytic redundancy relations) and flags (used as validity parameters for monitoring functions) are generated, then the variables are individually monitored by parameter monitors (e.g. for limit violations or against expected values) and afterwards the states of the different parameter monitors can be logically combined in the functional monitoring to realize more specific detection possibilities. If a monitoring event (e.g. a limit violation of a parameter) with an associated reaction occurs, a so-called recovery command is send which triggers the execution of the recovery action.

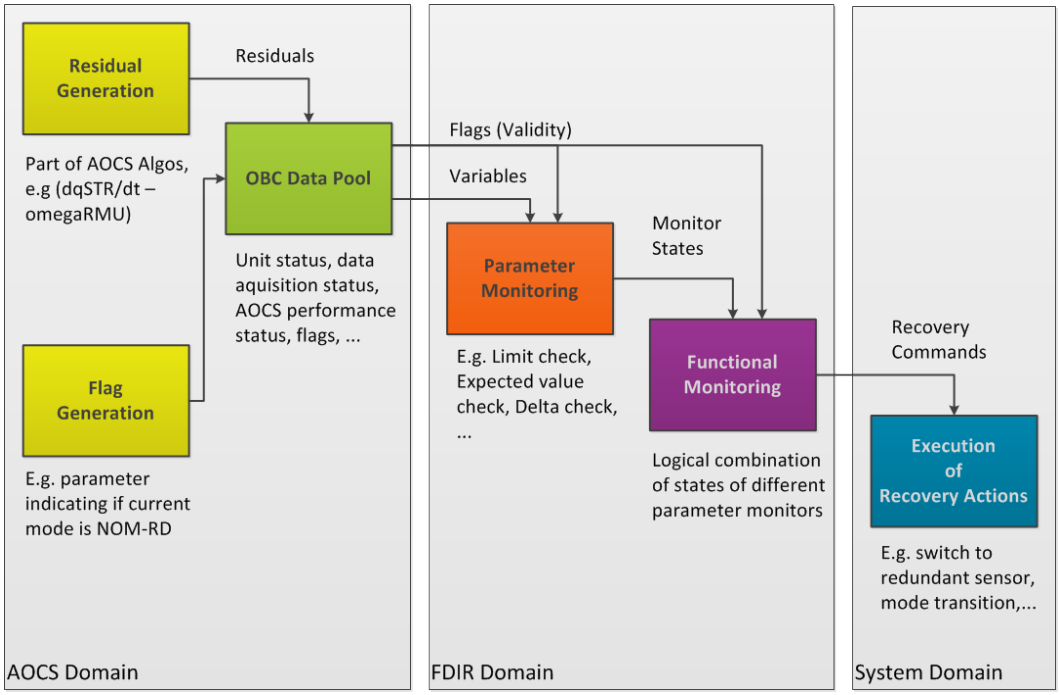


Figure 4-11: Typical FDIR information flow.

### 4.3.1 Definition of Operational States of AOCS Equipment

The functional chains of the AOCS usually depend on a great number of involved units (sensors and actuators). Each unit can be in different operational states and each state is connected to different monitoring functions to be executed in order to obtain an estimate of the proper functioning of the unit. Therefore it is very important for a systematic FDIR to model the operational states of different units in a generic way.

Figure 4-12 illustrates a generic behavioral model for AOCS units (sensors and actuators) that covers the most important states in the context of FDIR. The state hierarchy is the following: A unit can either be “Off” or “Powered”. If it is powered it can be in “Standby”, “Initializing” or “Operational” state. In operational state, the intended function (e.g. to measure something or to apply forces or torques) can be provided either with “Full Performance”, “Reduced Performance” or the intended function can be “Suspended”. If the behavioral states of every AOCS unit are abstracted in such a way, the monitoring of the different states can be performed in a very systematic way.

The definition of the used states is:

- Off (OFF): The unit is not powered, i.e. does not communicate, is not operational.
- Powered: The unit is powered and…
  - Standby (STB): not communicating, not operational
  - Initialization (INI): communicating, not operational



Doc.No.: GAFE-UM-D7.5a
Issue: 2.0
Date: 13.06.2018

- Operational: communicating, operational
  - Suspended (SUS): measurement/actuation is suspended (e.g. star tracker blinded)
  - Reduced Performance (RP): measurement/actuation ok, but coarse (e.g. track tracker at high rate)
  - Full Performance (FP): measurement/actuation with full performance
- Test (TST): A dedicated mode for self-testing, calibration, etc. The unit is communicating, but is not considered operational.

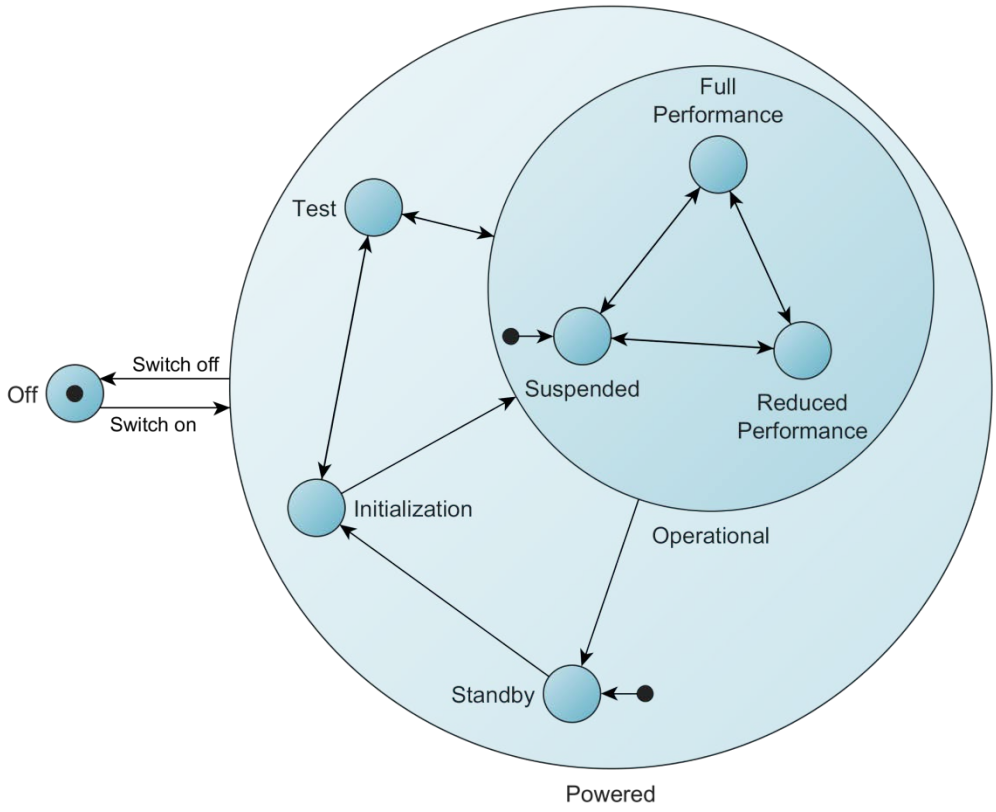


Figure 4-12: A generic behavioral model for AOCS units (sensors and actuators).

This generic behavioral model can be used as template to derive individual models for each type of AOCS equipment on-board the spacecraft.

This derivation consists of the tasks to determine:

- which states are representative for a specific unit (and to remove the other ones)
- which state transitions are representative (and to remove the other ones)
- of which type the state transitions are. Either manual (M), i.e. by TC from system/ground, or automatic (A)

- how long the transitions typically take, e.g. A(3) for an automatic transition which takes 3 seconds.

The specific behavioral model of each unit can then be expressed by a state transition table similar those in Table 4-8 or Table 4-9.

Table 4-8: Exemplary state transition table of star tracker with a test mode.

| State | | From | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | OFF | STB | INI | TST | SUS | RP | FP |
| To | OFF | M | M | M | M | M | M | M |
| | STB | M(3) | M | | | | | |
| | INI | | A(10) | M | M | | | |
| | TST | | | M(3) | M | M(3) | M(3) | M(3) |
| | SUS | | | A(1) | M | M | M | M |
| | RP | | | | | M | M | M |
| | FP | | | | | M | M | M |

Table 4-9: Exemplary state transition table of a simple magnetometer.

| State | | From | |
|---|---|---|---|
| | | OFF | FP |
| To | OFF | | M |
| | FP | M | |

### 4.3.2 Definition of Model-Based Residuals

The results from the structural analysis performed in task 2 (see Section 4.2) for the final system configuration are:

- Fault detectability and isolability information
- Fault signatures/residual structure

The residual structure tells the user, which known states (commanded or sensed variables) are part of which residual. Starting with this information, the user then has to pick/find the mathematical model for the residual and implement it. The mathematical models are based on the real world relations which were fed as part of the qualitative system model to the structural analysis. Some of the real world relations are listed in Table 4-10 and information on their possible implementation as mathematical model can be found in [RD-3].

Table 4-10: Real world relations for potential residuals and qualitative computational effort.

| Real World Relation | Relation Between States | Computational Effort |
|---|---|---|
| Attitude Kinematics | attitude, rate | low |
| Attitude Dynamics | rate, torque, inertia | low |
| Position Kinematics | position, velocity | low |
| Position Dynamics | velocity, force, mass | low |
| Relative Motion | relative position, relative velocity, relative acceleration | low |
| Sun Direction | sun direction, time, position, attitude | medium |
| Earth Direction | earth direction, time, position, attitude | medium |
| Magnetic field | attitude, position, time, magnetic field vector | medium/high |
| Reaction wheel torque | wheel command, wheel torque, wheel rate | medium |
| Magnetorquer torque | mtq command, mtq torque, magnetic field vector | medium |
| Thruster force and torque | thruster command, thruster torque, thruster force | medium/high |

### 4.3.3 Definition of Observables

The term observable is used in the context of this methodology to summarize all kind of information stored in the OBC data pool that it is likely to change during flight (independently of the frequency of change) and that is available for monitoring purposes.

Observables can be roughly divided into two groups:

- Variables (parameters[2]): e.g. the current spacecraft rate measured by RMU1 or the value of a timeout counter. Variables are often monitored for limit violations or against defined expected values. They can be of different data type, like e.g. boolean, integer, floating point.
- Flags (validity parameters[3]): e.g. a flag indicating if the AOCS is currently in the sub-mode “Rate-Damping (RD)” of its “Acquisition and Safe Mode (ASM)” (isAocsModeAsmRd). The data type of flags is boolean.

Parameter monitoring normally uses both type of information. Example: “If the current AOCS mode is ASM-RD, the spacecraft rate measured by RMU1 shall be monitored against limit

[2] In the context of software and FDIR all items in the OBC data pool are often just called parameters. Therefore the term parameter is used as synonym for variable.
[3] In the context of FDIR the purpose of flags is often to serve as so-called “validity parameters” for monitoring functions. The term validity parameter is described in the PUS-Standard of Service 12: „The associated validity parameter“ … „is a Boolean parameter whose value determines whether the parameter is monitored“. The terms flag and validity parameter are used here interchangeably.

violations of +/-4°/s. Then the spacecraft rate is the variable to be monitored (here checked for limit violations) if and only if the flag (validity parameter) “isAocsModeAsmRd“ is true.

To create a complete and precise list of all observables to be available in flight for monitoring is a key element of a good FDIR concept. The most important kinds of information which should be made available as observables for monitoring purposes are summarized in the following sub-sections.

#### 4.3.3.1 Variables (Parameters)

The following types of variables should be made available to the FDIR for monitoring purposes:

- Equipment related:
  - Quantities allowing to determine the real status of each AOCS unit regarding:
    - Real power status: e.g. a current measurement from the PCDU
    - Real communication status: e.g. a flag from data handling telling whether the formal communication with a unit is working (e.g. available TM packets, TC acknowledgements, response time ok, CRC ok)
    - Real operational status: e.g. a flag from the AOCS sensor processing telling if e.g. the measurements of a sensor are within reasonable ranges, the time stamps of the packets are increasing, there are no large jumps between consecutive measurements, no frozen/stale data, etc.
    - Housekeeping information: e.g. temperatures
    - Status information resulting from unit self-tests
- Equipment Management related
  - Duration of unit activation or unit mode transition
  - Availability of sufficient equipment to
    - Maintain current AOCS mode
    - Prepare upcoming AOCS mode
- Mode Management related:
  - Elapsed time of activities or transitions
    - currently prepared
    - currently performed
- AOCS related:
  - Values, absolute values and/or errors of
    - Attitude of spacecraft (e.g. to check pointing errors)
    - Angular rate of spacecraft
    - Orbital parameters (e.g. Kepler elements)
    - Angular rate and momentum of reaction wheels (assembly and single wheels)
    - Relative states between multiple spacecraft (e.g. for RvD and FF)

- States (e.g. angles) of solar array drive mechanism, antenna pointing mechanism, …
- Eclipse information
- Performance figures and timers of AOCS algorithms, e.g. estimated error of orbit propagator, time since last measurement update of orbit propagator, innovation of sensor fusion filters, estimated friction of reaction wheels
- Slew/transition durations (before being in steady state)
- Residuals derived by means of analytic redundancy relations
- Instrument exclusion zones (e.g. Sun, Earth, Moon)

#### 4.3.3.2 Flags (Validity Parameters)

The following types of information should be made available to the FDIR as flags in order to serve as “validity parameters” for monitoring functions:

- Current AOCS mode, submode, and mode/sub-mode combination
  - Usually provided by AOCS mode manager
- Desired AOCS mode and submode
  - Mode under preparation for planned transition
- The expected status of each AOCS unit provided by the equipment management function of the satellite
  - Expected power status: i.e. if unit is supposed to be powered or not
  - Expected communication status: i.e. if unit is supposed to provides telemetry and is accepting telecommands
  - Expected operational status: i.e. if unit is supposed to be operational or not
    - Operational for sensor functions means: sensor is able to provide measurements if environmental conditions allow (a blinded star tracker is still operational, a sun sensor with the Sun out of its field of view, too)
  - Expected usable status (whether a unit is supposed to be used in the AOCS closed loop and/or in the AOCS FDIR). A unit is expected to be usable if it is foreseen to be used in the current AOCS mode (defined by parameter) and its expected operational status is “operational”.
  - Expected test status: i.e. if the unit is supposed to be in test mode
    - This information is important for the activation of monitoring functions that evaluate the result of unit self-tests.
- Flags indicating that an activity or transition (e.g. AOCS mode and submode) is
  - currently prepared (e.g. enabling additional equipment)
  - currently performed (e.g. transition from inertial pointing to nadir pointing)

Best practice requirement(s) related to observables are:

- FDIR-BP-503: No fault management function shall trigger on test data generated by a unit operating in test mode.
- FDIR-BP-504: Entering a test mode shall not require (or imply) disabling of fault management functions.

If unit test modes are modelled separately from operational modes (as proposed in section 4.3.1) the best practice requirements FDIR-BP-503 and FDIR-BP-504 can be easily fulfilled by connecting the validity of monitoring functions for test evaluation and operation on the corresponding status flags.

### 4.3.4 Definition of Considered Equipment Failures and Feared Events

In a typical FDIR hierarchy (see Figure 4-13) the AOCS is located on the application level (level 2), which is one level above the unit/equipment level (level 1) and one level below the system or satellite level (level 3). The perimeter of the AOCS related FDIR normally spans between these three levels (indicated in yellow in Figure 4-13). From this perspective the AOCS FDIR has to deal with failures in the AOCS equipment and with failures of the AOCS itself. Failures of AOCS equipment are addressed in Section 4.3.4.1 in a bottom up approach; failures of the AOCS on the other hand are addressed as feared events in Section 4.3.4.2.

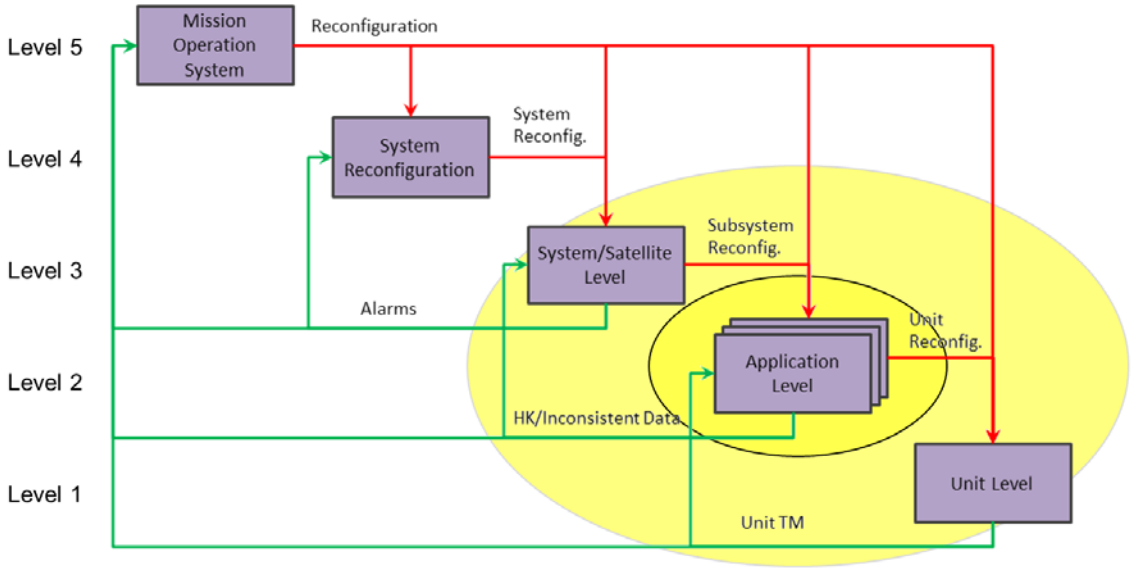


Figure 4-13 Hierarchy of generic FDIR system for Spacecraft.

#### 4.3.4.1 AOCS Equipment Failures

Failures of different AOCS units (sensor and actuators) are typically known from experience for well-known and space proven units, or derived from reasoning or test for new kind of units. Since the system boundary of an AOCS unit can be clearly defined, the failure of an AOCS unit can be considered as fault to the AOCS (see definition of fault and failure in Section 7.2.1). A typical analysis to deal with unit failures is the failure mode, effect (and criticality) analysis

(FME(C)A), see Section 6.1). In contrast to the feared event approach for the overall AOCS (see Section 4.3.4.2) the FME(C)A is a bottom-up analysis.

The following tables list anomalies, faults & failure for different types of AOCS units derived from in-orbit experience. The tables can serve as templates for the generation of a mission specific list of considered equipment failures and the following generation of an FME(C)A.

Table 4-11: List of credible failures for star trackers (STR).

| Failure | Description/Example |
|---|---|
| Complete failure | Loss of unit (e.g. due to short circuit, failure of ICs, ...) |
| Communication failure | Loss of communication (e.g. due to SEU) |
| Self-test failure | Failure in build-In self-test |
| Stale data | Unit delivers unchanged telemetry over and over again |
| Bias | Jump in measurement bias (e.g. due to moon in FoV, variable index of confidence) |
| Temperature | Temperature increase leading to loss of measurement |
| Bright Object | Permanent "Bright Object in FoV", but measurement ok (due to SEU, gone after restart) |
| Erroneous quaternion | Erroneous quaternion, e.g. element of quaternion frozen to 1 (due to SEU, gone after restart), or norm of quaternion significantly different to 1. |
| Reboot | Undesired reboot (with/without stucking in boot-mode) |
| Overcurrent | Overcurrent (leading to LCL based switch-off) |
| Unexpected blinding | Long term unexpected blinding (e.g. due to very strong solar flare) |
| Mode lock | Lock in certain operational mode (e.g. tracking) |
| Unexpected mode transition | E.g. permanent fall back from attitude update mode to initial acquisition mode |

Table 4-12: List of credible failures for Rate Measurement Units (RMU).

| Failure | Description/Example |
|---|---|
| Complete failure | Loss of unit (e.g. due to short circuit, failure of ICs, ...) |
| Communication failure | Loss of communication (e.g. due to SEU) |
| Self-test failure | Failure in build-In self-test |
| Stale data | Unit delivers unchanged telemetry over and over again |
| Drift | Jump in drift (OoM: 1°/h) |
| Noise | Noise increase (over full spectrum or e.g. only low frequencies) |

| | |
|---|---|
| Temperature OoR | Temperature Out of Range |

Table 4-13: List of credible failures for Global Navigation System Receiver (GNSR).

| Failure | Description/Example |
|---|---|
| Complete failure | Loss of unit (e.g. due to short circuit, failure of ICs, ...) |
| Communication failure | Loss of communication (e.g. due to SEU) |
| Self-test failure | Failure in build-In self-test |
| Stale data | Unit delivers unchanged telemetry over and over again |
| Time error | Jump of measured GPS time |
| Position error | Jump of measured position (OoM: 100m) |
| Outage | Erratic loss of PVT |
| Reboot | GPSR reboot |
| No convergence | No convergence of GPS after (re)start |
| Delayed convergence | Delayed convergence of GPS after (re)start (OoM: 10h) |

Table 4-14: List of credible failures for Reaction Wheels (RW).

| Failure | Description/Example |
|---|---|
| Complete failure | Loss of unit (e.g. due to short circuit, failure of ICs, ...) |
| Communication failure | Loss of communication (e.g. due to SEU) |
| Tachometer bias | Error in measured wheel speed (due to SEU, OoM: 10 rpm, gone after restart) |
| Temperature measurement error | Wheel temperature measurement error (e.g. outlier due to SEU, gone after restart) |
| Magnetic noise | Increased magnetic noise (visible in magnetometer measurement?) |
| Friction & Temperature increase | Wheel temperature increase due to jump/variation of friction (e.g. due to degradation of lubricant, cage instability) |

Table 4-15: List of credible failures for Reaction Control System (RCS)

| Failure | Description/Example |
|---|---|
| Vapor lock/bubbles (force/torque) | Disturbance force/torque during maneuver (due to vapor lock or bubbles) |
| Vapor lock (non-response) | Random non response of one/several thrusters (due to vapor lock) |
| Leakage | Pressure decrease/drop resulting in lower force/torque (for blow down system) or decreasing pressure measurements for |

| | |
|---|---|
| | pressure regulated systems. |
| Long burn | Thrust variation during long burns |

Table 4-16: List of credible failures for Solar Array Drive Electronics (SADE)

| Failure | Description/Example |
|---|---|
| Complete failure | Loss of unit (e.g. due to short circuit, failure of ICs, ...) |
| Communication failure | Loss of communication (e.g. due to SEU) |
| Stale data | Unit delivers unchanged telemetry over and over again |
| Position measurement jump | Jump in measurement of angular position (OoM: 50°) |

#### 4.3.4.2 AOCS Feared Events

Bottom-up approaches like FME(C)A (see) help to cover potential unit failures in the FDIR design. Complementary to this bottom-up approach is a feared event analysis asking the question: what kind of situation is critical for the spacecraft, the payload, etc. and how can it happen. The feared events are then broken down (e.g. by means of a fault tree, see Section 6.2) into more elementary items, which can be handled individually (e.g. by providing detectability and isolability for a certain unit failure or by including a sufficient number of items to recover from a failure of such an elementary item). This kind of analysis also helps to identify so-called vital equipment, i.e. equipment that is absolutely essential for safe/survival mode.

The Catalogue of Failure Data for Safety and Dependability Analysis (see [RD-7]) has the goal to become a framework for the effective support to safety & dependability analysis in the future. Some of the items below have been taken from there.

Table 4-17: List of feared events for the AOCS

| Feared Event | Description/Example |
|---|---|
| Payload/Platform Blinding | Blinding of optical instruments, e.g. telescope looking into the Sun. |
| Spacecraft Collision | For rendezvous and docking or formation flying missions |
| Spacecraft Rate | Spacecraft rate error exceeds maximum expected values |
| Spacecraft Attitude | Spacecraft attitude error exceeds maximum tolerable values (e.g. in terms of pointing error, oscillation, etc.) |
| Reaction Wheel Angular Momentum | Reaction wheel angular momentum exceeds maximum expected values |
| Mode Convergence | Critical AOCS mode does not converge to target<br>e.g. rate damping, sun acquisition or earth acquisition |
| Slews Convergence | Attitude slews do not converge |

| | |
|---|---|
| Consumables | Excessive thruster usage, excessive battery use |
| Loss of GNSS | Loss of GNSS information (time, position, velocity) |
| Reboot | Reboot of on-board computer |
| Maneuver Failure | RCS or AOCS failure during orbit maneuver |
| Orbit Propagator | Orbit propagator update time-out or invalid |
| No/Wrong Acquisition | No or wrong acquisition of bright object (e.g. moon instead of sun) |
| Overheating of spacecraft elements | Exposing of radiators or thermally sensitive spacecraft side to Sun or hot planet |

### 4.3.5 Definition of Monitoring Functions

State-of-practice monitoring functions for spacecraft can be grouped in two groups:

- Parameter Monitors
- Functional Monitors

#### 4.3.5.1 Parameter Monitoring

The parameter monitoring is the first stage of FDIR monitoring and consists of a set of different parameter monitors (realized often by means of PUS Service 12). Every parameter monitor looks only at a single variable (parameter) and checks it (or its gradient) either against lower and upper limits (for floating point or integer variables) or against an expected value (for integers or booleans).

Additional attributes of each parameter monitor are the monitoring frequency (usually specified as multiple of the sampling frequency of the associated application software, in our case the AOCS software), the number of consecutive limit/expected value violations that lead to a change of the monitor's state, and eventually associated events to be triggered in case of a state change (e.g. below lower limit event).

Typical variables to be monitored are AOCS equipment states (e.g. if a unit is properly communicating or if it is providing valid measurements), performance figures (e.g. pointing error, spacecraft rate errors) or timers (e.g. elapsed time since start of a mode transition).

A detailed list of variables typically surveyed by parameter monitoring can be found in the section 4.3.3.1. The most common flags to make the execution of individual parameter monitors depend on can be found in section 4.3.3.2.

The monitoring frequency, number of consecutive violations, limits etc. are very specific and must be defined for every project individually.

Best practice requirement(s) related to parameter monitoring are:

- FDIR-BP-101: FDIR shall not trigger on one sample of a parameter. Possibly redundant readings shall be verified. As a minimum, contiguous samples shall be used.
- FDIR-BP-113: The fault management shall include monitoring of individual equipment measurements (e.g. time stamp updates, validity flags, measurement ranges) to detect corrupted or old data.

#### 4.3.5.2 Functional Monitoring

For simple equipment faults (e.g. a unit delivers no telemetry at all) the corresponding fault signatures are mostly atomic, i.e. that such faults can often be detected and isolated by looking with a single parameter monitor on a specific indicator (in the no telemetry example e.g. on a flag expressing the current communication status of the unit). For such cases pure parameter monitoring is sufficient and often straightforward to define.

For more complex faults (e.g. a continuous drift in the rate measurement of the RMU) the corresponding fault signatures are not straightforward and often involve multiple indicators to be looked at for detection and especially isolation. In this case so-called functional monitoring is used to logically combine the observations of multiple parameter monitors in order to detect anomalies.

The structural analysis described in Section 5 is able to provide fault signatures for all investigated faults. These signatures (see Section 5.6) can be used to set up corresponding functional monitors.

In principle functional monitoring has always been used in form of hard coded functions in the flight software. The advantage of using a dedicated service (like e.g. a PUS service) for it is the higher flexibility when it comes to updates of the monitoring functions (e.g. adding an additional condition to be checked for a functional monitor) or the need to add additional ones.

### 4.3.6 Definition of Recovery Actions

Classical recovery actions performed to recover from an AOCS related faults can be categorized as follows:

- Parameter adaptation
- Equipment reconfiguration
- System reconfiguration

If successful, the first two lead to a continuation (or at least quick restoration) of the desired operational state of the spacecraft (fail-operational approach), whereas the last one leads to a transition to a safe state (Fail-Safe approach). However, it is noted that fail-operational FDIR can be achieved even including total system reconfiguration. This is achieved by immediate switch-over to the hot-redundant branch, including the on-board computer also, with system context switching allowing continuation of the current operation. This is the ultimate way of

implementation of fail-operational FDIR design and which is the only choice for missions with very stringent/demanding requirements on operational outage.

Note that the term “operational outage” is used above in the widest sense and can represent abortion of delta-V manoeuvre or payload outage or mission loss etc.

Important aspects for recovery actions are possible constraints they must comply with. Typical constraints are:

- Time to recovery: the maximum time span the recovery (unit reconfiguration or system reconfiguration) is allowed to last.
- Performance envelopes: e.g. envelopes for attitude (error), rate (error), angular momentum, velocity etc. that must not be left or not be entered during recovery (fail-operational scenario).
- Initial conditions: for system reconfigurations with transition to safe mode the acceptable initial conditions of the safe mode (e.g. the maximum spacecraft rate or angular momentum at safe mode entry) need to be respected (fail-safe scenario).

In the verification of the FDIR concept such constraints need to be explicitly checked for violations.

Best practice requirement(s) related to recovery actions are:

- FDIR-BP-204: It shall be possible to reconstruct from telemetry the conditions leading to the generation of an event.
- FDIR-BP-203: Anomalies and actions taken to recover from them shall be reported in event driven packets.

#### 4.3.6.1 Parameter Adaptation

Parameter adaptations in the AOCS algorithms can be used as mean to continue operation under changed conditions caused by a fault. Corresponding fault tolerant control concepts require a precise isolation of a fault and a reliable estimate of the parameters that have changed due to the fault.

An example for parameter adaptation would be the online update of the force/torque distribution function for a reaction control system in case of degradation of a single thruster.

#### 4.3.6.2 Equipment Reconfiguration

If the failure of a specific unit has been detected and isolated (by means of monitoring functions), one of the following lists of actions need to be performed

- Unit restart consisting of
  - unit software restart and/or power cycling
  - decrement of health status of unit (in order to avoid endless restarts)

- Unit reconfiguration (in case unit restart is not desired or was not successful):
  - exclusion of failed unit from the set of AOCS units used for closed loop control
    - in case of actuators: send “zero-actuation” command before exclusion (especially if the unit is not directly switched-off for investigation reasons)
  - set health status of the unit to failed
  - activate adequate substitute for the failed unit
  - include substitute into the set of used AOCS units for closed loop control
  - if no adequate substitute is available (i.e. no healthy unit or valid configuration available) this needs to be reported to AOCS’ parent FDIR level (usually system level with the consequence of a system reconfiguration).

Both concepts (restart and reconfiguration) required potentially a reset or re-initialization of dynamic AOCS software functions, e.g. of:

- filters states (e.g. for measurements acquisition, residual generation)
- controllers states
- residual generators states
- actuation algorithms states (e.g. sigma-delta loop)
- selections functions states (e.g. sensor selection 1 of 3)
- local FDIR monitoring functions states (e.g. invalid counters)

In order to handle equipment reconfiguration in a systematic way, two basic concepts have proven useful:

- Unit Health Table (UHT)
- Equipment Configuration Table (ECT)

#### 4.3.6.2.1 Unit Health Table

The health status of all units can be expressed by integer numbers stored in a so-called Unit Health Table (UHT). A positive health status number indicates a healthy unit, a health status equal to zero indicates an unhealthy (failed) unit. The initial health status of all units has to be defined by the FDIR engineer. Every health status greater than one indicates the number of attempts the equipment manager shall make to restart a unit in case an anomaly or failure was detected in it.

In the exemplary health status table shown in Figure 4-14 the fourth reaction wheel is already marked to be unhealthy (i.e. no restart attempt), but all rate measurement units and three out of four star trackers would be restarted once after a failure and their health would be reduced by one. All other units would be directly marked unhealthy after a failure (with no restart attempt).

| Equipment | Unit 1 | Unit 2 | Unit 3 | Unit 4 | Unit 5 | Unit 6 |
|---|---|---|---|---|---|---|
| Digital Sun Sensor | 1 | 1 | 1 | 1 | 1 | 1 |
| Magnetometer | 1 | 1 | 1 | N/A | N/A | N/A |
| Star Tracker | 2 | 2 | 1 | 2 | N/A | N/A |
| Rate Measurement Unit | 2 | 2 | N/A | N/A | N/A | N/A |
| ... | ... | ... | ... | ... | ... | ... |
| Reaction Wheel | 1 | 1 | 1 | 0 | N/A | N/A |
| Reaction Control System | 1 | 1 | N/A | N/A | N/A | N/A |

Figure 4-14 Exemplary Unit Health Table showing health status of AOCS equipment

#### 4.3.6.2.2 Equipment Configuration Table

The Equipment Configuration Table (ECT) contains valid configurations of AOCS units and is very useful to define allowed and preferred configurations for equipment reconfiguration.

An exemplary equipment configuration table for one AOCS mode and three different AOCS equipment types is illustrated in Figure 4-15. Each row per equipment indicates a valid configuration of the units of that equipment. If one unit fails (i.e. the corresponding entry in the UHT turns zero), all configurations which include this unit become invalid. The equipment reconfiguration task is then to pick the first valid configuration that provides the desired number of units for the current AOCS mode.

The color behind the configuration number (to the left of each row) expresses to which extend the configuration in this row is sufficient to perform all AOCS and AOCS related FDIR tasks in the current AOCS mode. “Green” indicates that if all marked (table entry “1”) units of a certain equipment are operational, all AOCS and FDIR functions can work well. “Orange” indicates that the nominal AOCS functions can be performed, but the operational units are not sufficient to perform all FDIR functions (e.g. different faults could not be unambiguously traced back to a single failed unit, i.e. full isolability not possible). The last configuration row of each equipment type is marked “Red”, meaning that even the AOCS functions cannot work as intended with the remaining units. If there is no valid configuration above the red one, equipment reconfiguration is not sufficient to restore the desired mode of operation and a higher level FDIR reaction is required (e.g. system reconfiguration).

The general ECT concept is very flexible and allows e.g. to define groups of units which need to operate together: e.g. two sensor groups where each group provides a spherical field of view. If one unit of one group fails, the ECT can be parameterized such that the equipment management function would switch over to the other group.

Equipment 1

| Config | Unit 1 | Unit 2 | Unit 3 | Unit 4 |
|---|---|---|---|---|
| 1 | 1 | 1 | | |
| 2 | 1 | | 1 | |
| 3 | 1 | | | 1 |
| 4 | | 1 | 1 | |
| 5 | | 1 | | 1 |
| 6 | | | 1 | 1 |
| 7 | 1 | | | |
| 8 | | 1 | | |
| 9 | | | 1 | |
| 10 | | | | 1 |
| x | * | * | * | * |

Equipment 2

| Config | Unit 1 | Unit 2 | Unit 3 |
|---|---|---|---|
| 1 | 1 | 1 | |
| 2 | 1 | | 1 |
| 3 | | 1 | 1 |
| 4 | 1 | | |
| 5 | | 1 | |
| 6 | | | 1 |
| x | * | * | * |

Equipment 3

| Config | Unit 1 | Unit 2 | Unit 3 | Unit 4 |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | |
| 2 | 1 | 1 | | 1 |
| 3 | 1 | | 1 | 1 |
| 4 | | 1 | 1 | 1 |
| x | * | * | * | * |

Figure 4-15 Exemplary equipment configuration table (ECT) for three equipment types

Best practice requirement(s) related to unit reconfiguration are:

- FDIR-BP-110: Where possible, failure recovery actions shall first attempt a software reboot before considering a hardware reconfiguration of the affected units.
- FDIR- BP-108: The spacecraft shall maintain a list of available, suspected and failed hardware units. This information shall be updatable by dedicated telecommand and available in telemetry.

#### 4.3.6.3 System Reconfiguration

There are different reasons that might lead (by design) to a reconfiguration of the complete spacecraft, a so-called system reconfiguration. Examples are that OBC software elements do not finish their tasks in the foreseen time frame (watchdog timer), there occurred a SEU or hardware failure in the OBC, there was a power drop, or a performance figure of the AOCS (like e.g. spacecraft rate or attitude error) is inexplicably out of bounds (i.e. the FDIR had not detected any specific failure except the violation of these bounds).

A system reconfiguration is usually linked to a restart of the on-board computer (OBC) and includes many items to be defined in order to start the system up in a well-defined way:

- Which OBC processor module (and reconfiguration module) shall be used? The same or a redundant one
- Which software image shall be used (from which memory)?
- Is it an OBC restart or only a software restart (different delays)?
- Which avionic chain/AOCS equipment configuration shall be used?
- Shall the AOCS equipment be power-cycled or not?
- Which AOCS mode shall be entered after restart (e.g. same as before or directly a safe mode)
- Which context information, e.g. for operations and AOCS, shall be reused (e.g. last GPS PVT, date and time, health status of equipment)?
- Shall the FDIR be changed after restart?

Usually, a table of different system configurations is stored in a non-volatile SGM EEPROM memory of the spacecraft together with the number of the current system configuration. At initial start of the OBC the first configuration is used, for every further restart of the system the configuration to be used is also defined in the table. However, SGM EEPROM has a limited number of write-cycles they are qualified for. Therefore, the information written into SGM EEPROM must be of type which does not change very often during the mission. The equipment configurations used after the different OBC resets is the prominent example to be stored into SGM EEPROM and which is only updated by ground. However, if information is intended to be used after an OBC reset which is e.g. cyclically stored into SGM by the software, the SRAM type SGM need to be used; which is volatile but has a much higher write-cycle qualification. A good example is e.g. the AOCS context information to be stored into SGM SRAM. This allows e.g. the current AOCS equipment configuration to be used directly after the OBC reset. Hence, besides the items listed above, it must be checked if dynamic AOCS software functions need to be additionally reset or re-initialized. This is typically the case when the AOCS context is re-established after the OBC reset.

Relevant items are e.g.:

- filters states (e.g. for measurements acquisition, residual generation)
- controllers states
- residual generators states
- actuation algorithms states (e.g. sigma-delta loop)
- selections functions states (e.g. sensor selection 1 of 3)
- FDIR monitoring states (e.g. invalid counters)

Table 2-4 gives an example of a system configuration table with the most important aspects to be defined by the AOCS FDIR responsible.

Table 4-18: Exemplary list of system configurations (system configuration table).

| System Config ID | Next System Config ID | Processor Module | Avionic Chain | Initial Aocs Mode | Units Power Cycling | Use Context Info | Enable FDIR |
|---|---|---|---|---|---|---|---|
| 1 | 2 | A | A | ASM | No | Yes | Yes |
| 2 | 3 | A | B | ASM | No | Yes | Yes |
| 3 | 4 | B | A | SAME | Yes | Yes | Yes |
| 4 | 5 | B | B | ASM | Yes | No | Yes |
| 5 | 6 | A | A | ASM | Yes | No | Yes |
| 6 | 1 | B | A | ASM | Yes | No | No |

Best practice requirement(s) related to system reconfiguration are:

- FDIR-BP-403: The transition to a safe mode, once started, shall not be interruptible.
- FDIR-BP-407: The spacecraft state variables shall be properly reinitialized for execution of the safe mode, and no residual values coming from previous spacecraft modes shall endanger the safe mode execution or recovery to normal mode.

### 4.3.7 Context Information

Define set of AOCS related context information to be stored in safeguard memory (in SRAM rather than in EEPROM). If desired (i.e. if use of context information is requested for current system configuration, see section 4.3.6.3) this information can be retrieved after a restart of the OBC or AOCS software. The following AOCS related items are safeguard memory candidates to be stored in SRAM:

- AOCS mode & sub-mode
- Used AOCS avionic chain (if used)
- AOCS equipment configuration
- Health status of AOCS units
- Deployment information (e.g. solar arrays, antennas, booms)
- Calibration information (e.g. star tracker absolute and relative alignment)
- Durations (e.g. elapsed time since entry into current mode, …start of deltaV maneuver, …last update of orbit propagator)
- Last valid attitude/rate measurement/estimate
- Last valid position/velocity/orbital elements measurement/estimate
- Eclipse information (e.g. max eclipse duration)

- For deep-space missions: e.g. distance to Earth, distance to Sun
- For RvD & FF missions: docking status, formation status
- Propellant estimate (impact on spacecraft mass, inertia, center of mass)

Best practice requirement(s) related to context information are:

FDIR- BP-114: Configuration and health status data shall be stored in safeguard memory.

FDIR- BP-112: If an on-board processor is switched from a main to a redundant unit (or vice versa), the switchover shall be such that operations can continue safely. Note: This implies that either the operational context need not be reloaded from ground, or the new processor can be loaded with a safe default context before the switchover.

## 4.4 Customization & Parameterization of GAFE Simulator (Task 4)

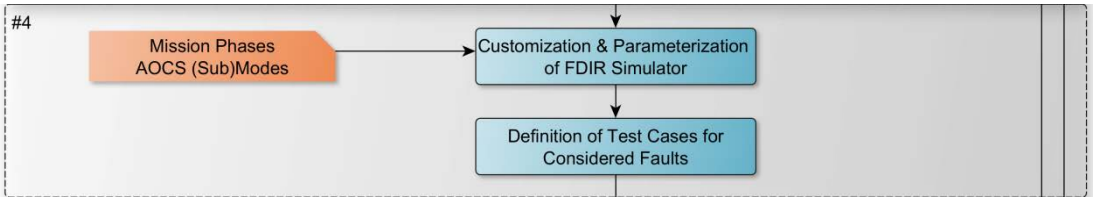


Figure 4-16 Elements of Task 4 (excerpt of high level flow).

The customization and parametrization of the GAFE Simulator is described in the User's Manual [RD-1]. The main steps are to configure the simulator such that it reflects the mission to investigated in the following points:

- Environment & Dynamics:
  - Spacecraft orbit
  - Time
  - Level of detail of physical & disturbance models
  - Spacecraft properties like mass, MoI, CoM, effective area, magnetic dipole, etc.
- Spacecraft:
  - AOCS equipment set
    - Alignment, sizing (e.g. 140 Am² MTQ, …), operational states and transition delays, …
  - AOCS algorithms
    - Sensor processing, determination/estimation, control, commanding, analytical models for FDI, residual generation, …
  - System level aspects:

- System configuration(s): which OBC processor module to use, avionic chain, context information, FDIR enable/disables, unit power cycling, initial AOCS mode, …
- AOCS modes, mode transition, entry modes,
- Required equipment configuration for each AOCS mode (and avionic chain)

- Faults
  - Which faults shall be considered: on equipment level and system level.
- FDIR
  - All kind of monitors and response actions.

## 4.5 Definition & Simulation of Test Cases (Task 5)

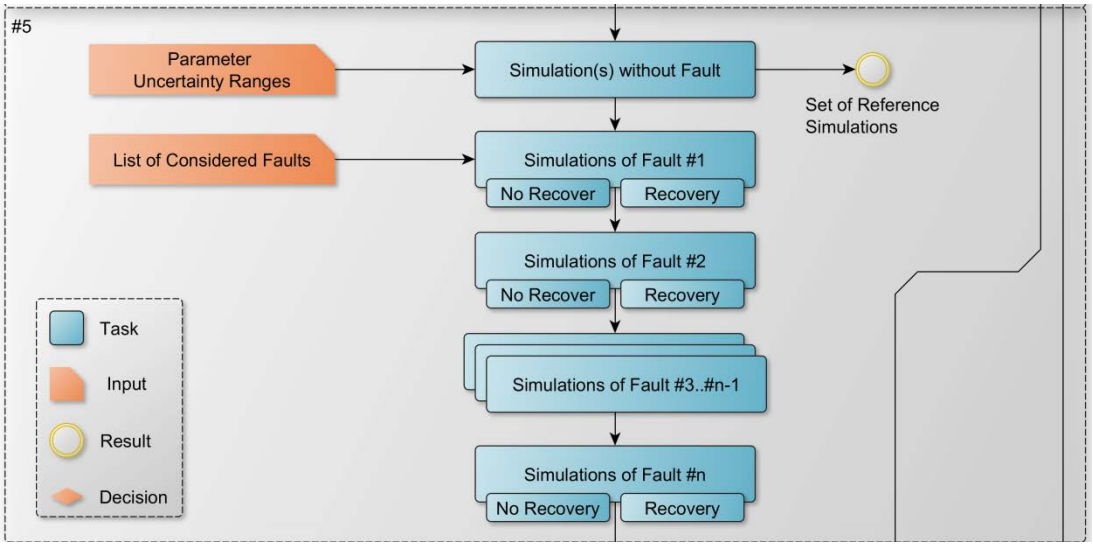


Figure 4-17 Elements of Task 5 (excerpt of high level flow).

The GAFE Simulator provides a very elegant concept for test case definition. Please refer to [RD-1], Section 4.3 and 4.4.2ff.

### 4.5.1 Definition of Test Cases

For each test case the following items have to be defined:

- System configuration
- Current AOCS Mode
- Fault(s) to be injected (time, type, persistency, etc.)
- Parameter uncertainty ranges
- How many runs in MC-Analysis

### 4.5.2 Simulation of Test Case

- Without fault,
- with fault
  - with recovery action
  - without recovery action

## 4.6 Evaluation of FDIR Performance (Task 6)

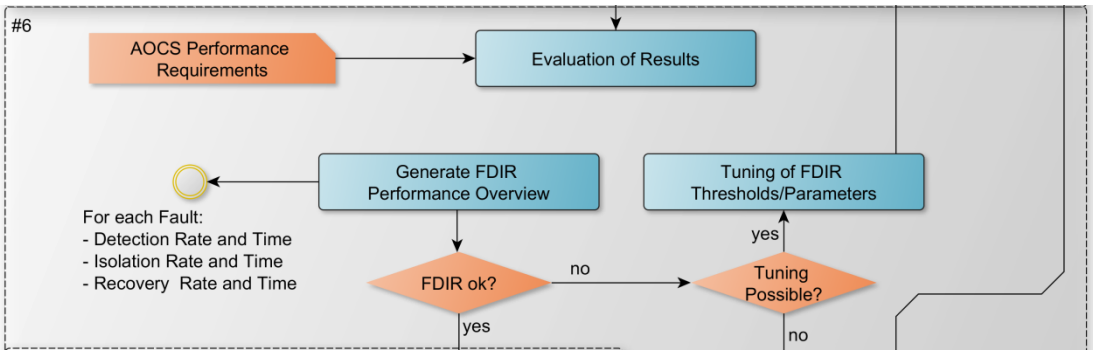


Figure 4-18 Elements of Task 6 (excerpt of high level flow).

As criteria to evaluate the performance of the FDIR under investigation the following items need to be checked:

- For Simulations without Faults:
  - Misdetections rate: were faults detected by the FDIR when no fault was present?
- For Simulations with Faults:
  - Was the injected fault detected at all?
  - How long was the time between fault injection and detection?
  - Was the injected fault isolated correctly (if required)?
  - If yes, it means that the fault was handled on the expected FDIR level.
  - Could the desired mode of operation be successfully held (fail-operational) or acquired (fail-safe) by the recovery action?
  - How long was the time between fault detection (and isolation) and successful recovery?

### 4.6.1 Evaluation of Test Cases

From the items above an FDIR Performance Overview can be generated from a set of test case data as shown in Table 4-19.

Table 4-19: FDIR Performance Overview.

| Failure | | Detection | | | Isolation | | Recovery | | |
|---|---|---|---|---|---|---|---|---|---|
| Test Case | Injected Fault | Correct | Status | Time [s] | Correct | Status | Procedure | Status | Time [s] |
| FDIR-001 | F1.01 | 20/20 | ok | [4.1…5.8] | 20/20 | ok | R1.01 | ok | [14.1…15.8] |
| FDIR-002 | F1.02 | 20/20 | ok | [4.4…6.2] | 20/20 | ok | R1.02 | ok | [16.4…19.2] |
| **FDIR-003** | **F1.03** | **17/20** | **nok** | **[3.2…7.4]** | 17/17 | ok | R1.03 | ok | [4.2…9.4] |
| FDIR-004 | F1.04 | 20/20 | ok | [4.4…6.2] | 20/20 | ok | R1.01 | ok | [16.4…19.2] |
| FDIR-005 | F1.05 | 20/20 | ok | [4.1…5.8] | 20/20 | ok | R1.02 | ok | [4.2…9.4] |
| FDIR-006 | F1.06 | 20/20 | ok | [4.4…6.2] | 20/20 | ok | R1.03 | ok | [6.4…13.2] |
| FDIR-007 | F2.01 | 20/20 | ok | [3.2…7.4] | 20/20 | ok | R2.01 | ok | [14.1…15.8] |
| **FDIR-008** | **F2.02** | **13/20** | **nok** | **[4.4…6.2]** | **4/13** | **nok** | **R2.02** | **nok** | **[16.4…19.2]** |
| FDIR-009 | F2.03 | 20/20 | ok | [4.4…6.2] | 20/20 | ok | R2.03 | ok | [4.2…9.4] |
| FDIR-010 | F2.04 | 20/20 | ok | [4.1…5.8] | 20/20 | ok | R2.01 | ok | [16.4…19.2] |
| FDIR-011 | F2.05 | 20/20 | ok | [4.4…6.2] | 20/20 | ok | R2.02 | ok | [4.2…9.4] |
| … | … | … | … | … | … | … | … | … | … |

## 4.7 Generation of FDIR Documentation (Task 7)

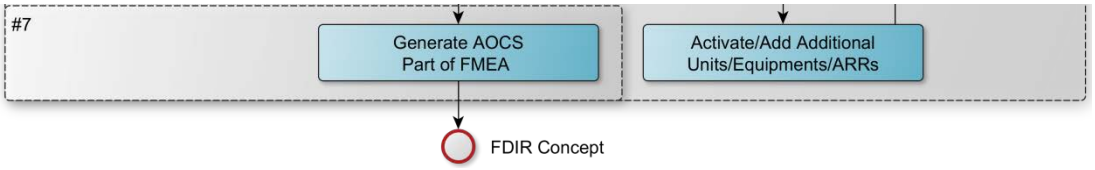


Figure 4-19 Elements of Task 7 (excerpt of high level flow).

If the methodology has been applied as described in the sections above, most information required by an AOCS related FME(C)A (Failure Modes and Effects, (and Criticality) Analysis) is already available. The list of considered faults and list of considered feared events are the basis for filling the FME(C)A (column “Failure Mode”). The other required items (according to [RD-4]) and the sources to take the information from are:

- Identification number:
  - unique, but arbitrary identifier
- Item/block:
  - The corresponding AOCS unit for unit faults or the AOCS subsystem for feared events
- Function:
  - Attitude (and Orbit) Control
- Failure mode:
  - From list of considered faults or list of considered feared events
- Failure cause:
  - So far not available, must be filled out manually
- Mission Phase/Operational Mode:

- AOCS mode(s) that use corresponding unit (from nominal AOCS design)

- Failure effect:
  - Locale & End effect: from simulation via violated AOCS requirement or manually
- Severity classification:
  - So far not available, must be filled out manually
- Observable symptoms:
  - Monitored observable(s)/fault signature
- Compensatory provisions:
  - Associated recovery action

Table 4-20: FMEA Worksheet according to [RD-4].

ECSS-Q-ST-30-02C
6 March 2009

**Failure Modes and Effects Analysis (FMEA)**

| **Product:** | | | **System:** | | | **Subsystem:** | | | **Equipment:** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ident. number | Item/ block | Function | Failure mode | Failure cause | Mission phase/ Op. mode | Failure effects a. Local effects b. End effects | Severity classification | Failure detection method/ observable symptoms | Compensating provisions | Recommendations | Remarks |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

# 5 Appendix A: Structural Analysis

## 5.1 Description

A very efficient approach for generation of the residuals called “Structural Analysis” is to analyze the structural model of the system (see [RD-5] and [RD-6]). This means to only take into account the structure of the constraints (which are treated as the links between states) and not the actual formula of the constraint itself. Obviously information is dropped in this process and therefore the resulting residuals have to be checked for feasibility later. It is possible to incorporate some constraint restrictions into the analysis, but these are only coarse (one-way-constraints, e.g. no integration, only differentiation possible).

The structure of a system can be represented as a bi-partite graph where an edge connects a state and a constraint. To work with the graph, this structure is noted in matrix form where the rows are the constraints and the columns are the states. Entries in the matrix represent the connections between states and constraints. The incidence matrix of the graph is described in more detail in section 5.2.

The incidence matrix is analyzed and shows the constraints carrying redundant information. Then these constraints are exploited to generate the residuals as described in section 5.5.

With knowledge about the available residuals it is possible to show detectability of faults and to determine if it is possible to localize individual faults by looking at the signature of the faults in the set of residuals as show in section 5.6.

### 5.1.1 System model

For a structured approach to FDI it is necessary to exploit the system model. In terms of the structural analysis the model consists of known and unknown states and constraints between these states.

### 5.1.2 States

The states can be separated into known and unknown ones.

The known states are variables whose values are inherently known, e.g. sensor readings. It has to be remarked that knowing these values does not mean to trust them.

Unknown states are variables which are more like states in a classical manner. These are internal states whose values are not known. The values of these unknown states can only be computed through constraints to known states.

### 5.1.3 Constraints

Constraints are links between states. The states can be known and/or unknown ones and there can be more than 2 states linked through a constraint. An example for a constraint is one that links the known state “GPS position measurement” to the unknown state “Current position”.

It is possible to have only unknown states in a constraint or mix between unknown and known states. Constraints which link only unknown states are called analytical constraints as they are some sort of model-based (e.g. kinematic relations). Constraints which link a known and an unknown state are called measurement constraints as they represent a sensor measurement.

### 5.1.4 Residuals

One method of FDI is to investigate a single variable and check for plausibility of the values (simple min/max tests and time-series analysis).

Another method of FDI is to detect discrepancies in variables connected to each other through constraints.

This leads to the definition of the residual, which is an equation based on several constraints linking only known variables together. In a fault free situation (neglecting noise) a residual has to be zero. If something is wrong in one of the known variables it will deviate from zero, which gives the possibility to detect the failure.

If a residual only involves measurement constraints, it is called a cross-check residual. If there are analytical constraints involved, the residual is called an analytical or model-based residual.

### 5.1.5 Fault Detection

To detect a fault it is necessary that the faulty state is observable. This means it is a requirement that the state is part of at least one residual. If this is the case it is possible to monitor this residual to detect an anomaly.

It is also important to have knowledge about how the fault affects the residual. E.g. a step like fault might become a peak in the residual through differentiation. Also it might be important to specify the nominal magnitude of the fault for some of the residual evaluation techniques.

### 5.1.6 Fault Identification

If a residual deviates from zero (neglecting noise), one of the states affecting this residual are faulty (under the assumption that only one fault can occur at a time). It can nothing be said about which one of the states is faulty as there is no redundant information contained in only one residual.

To further identify which one of the states is faulty it is necessary to have a number of residuals affected by these states. This yields the concept auf fault signatures, which describe which of the residuals are affected by one fault. If the signatures are unambiguous, the fault can be localized. This is described in more detail in section 5.6.

## 5.2 Structure Graph and Incidence Matrix

The structure of a system can be represented by a bi-partite graph with vertices from the set of constraints and the set of states. Each edge links one state with one constraint. The edges can be directed and the direction of an edge describes the direction of the relationship (state A →

constraint → state B means that state B can be calculated from state A, but state A cannot be calculated from state B).

An example is given in Figure 5-1: Constraint 1 links states A, B and C where each state can be calculated from the other two states. Constraint 2 links state B and D where state D can be calculated from state B but not vice-versa. Obviously this also describes the relation that state D can be calculated from states A and C by using constraints 1 and 2.

The known and unknown states (states A and B are known states, states C and D are unknown) are also marked in the graph.

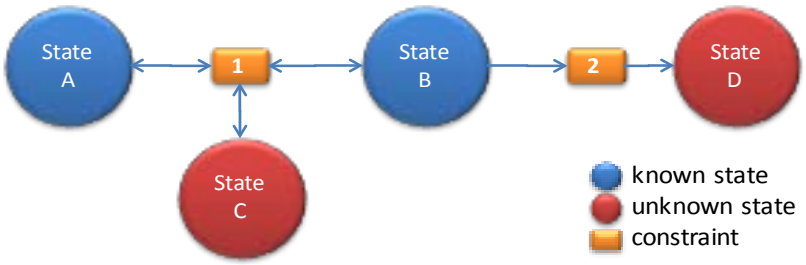


Figure 5-1: Simple structure graph

The incidence matrix represents the information contained in the structure graph in matrix form. The columns are the states and the rows are the constraints. The entries in the matrix mark links between states and constraints. Entries marked with a “1” show that it is possible to calculate this state with the constraint while entries marked with a “*” show that it is not possible although the state is part of the constraint. Table 5-1 shows the incidence matrix for the structure graph in Figure 5-1.

Table 5-1: Simple incidence matrix

| | | States | | | |
|---|---|---|---|---|---|
| # | Constraint | A | B | C | D |
| 1 | | 1 | 1 | 1 | |
| 2 | | | * | | 1 |

### 5.2.1 Exemplarily Application Case

Figure 5-2 shows the example structure graph for the sensor system components for the far-range approach phase of a rendezvous mission.

Known states (the sensor readings) are marked blue while unknown states (the “internal” states) are marked red. It can be seen that there are two subsystems without interconnection for this phase, namely the far range (FR) camera subsystem with the two far range cameras and the line of sight and the subsystem containing the rest of the sensors and states.

The incidence matrix for the structure graph shown in Figure 5-2 is given in Table 5-2. There are 15 constraints of which are 11 direct sensor measurements and 4 kinematic relations.

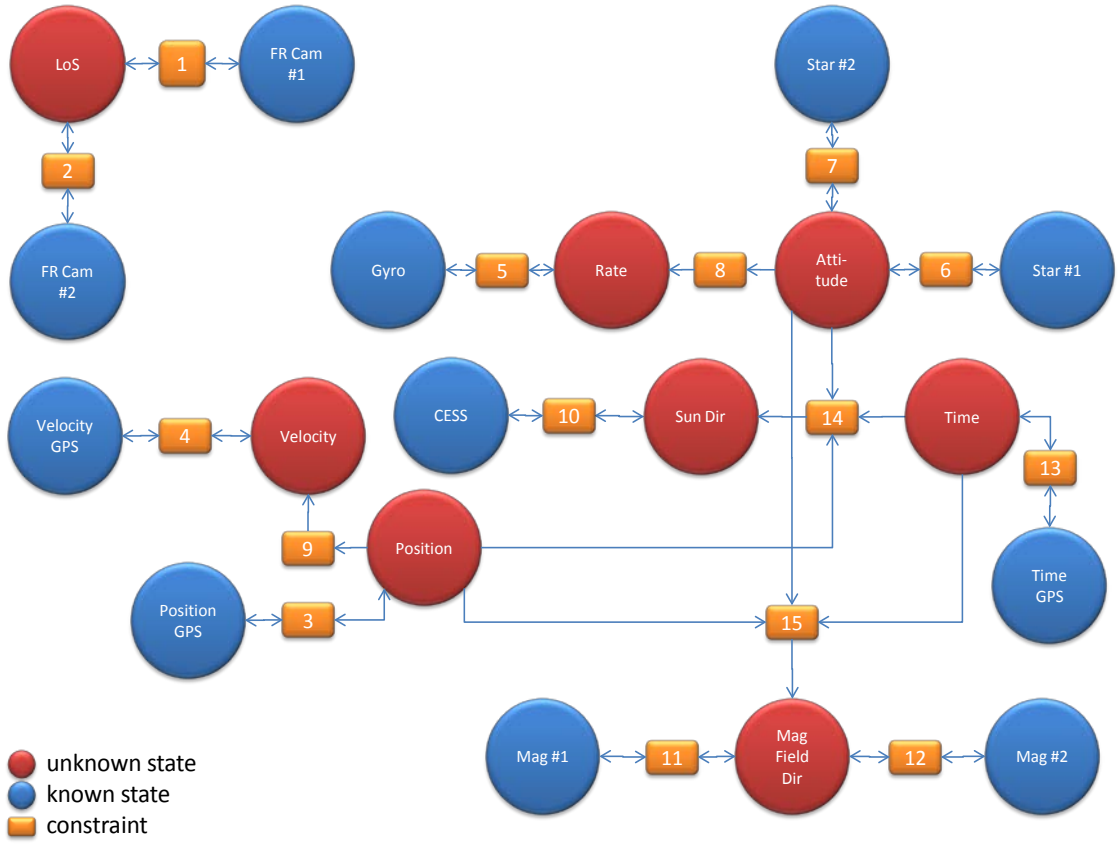


Figure 5-2: Structure graph of exemplarily setup

Table 5-2: Incidence matrix of exemplarily setup.

| | | Unknown states | | | | | | | | Known states | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Constraint | Line of sight to client | Time | Sun direction | Magnetic field direction | Inertial rate | Inertial velocity | Inertial attitude | Inertial position | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 |
| 1 | Los FR Cam #1 | 1 | | | | | | | | 1 | | | | | | | | | | |
| 2 | Los FR Cam #2 | 1 | | | | | | | | | 1 | | | | | | | | | |
| 3 | Position GPS | | | | | | | | 1 | | | | | 1 | | | | | | |
| 4 | Velocity GPS | | | | | | 1 | | | | | | 1 | | | | | | | |
| 5 | Rate Gyro | | | | | 1 | | | | | | | | | 1 | | | | | |
| 6 | Attitude star #1 | | | | | | | 1 | | | | | | | | | | | 1 | |
| 7 | Attitude star #2 | | | | | | | 1 | | | | | | | | | | | | 1 |
| 8 | Attitude derivative | | | | | 1 | | * | | | | | | | | | | | | |
| 9 | Position derivative | | | | | | 1 | | * | | | | | | | | | | | |
| 10 | CESS | | | 1 | | | | | | | | 1 | | | | | | | | |
| 11 | Mag #1 | | | | 1 | | | | | | | | | | | 1 | | | | |
| 12 | Mag #2 | | | | 1 | | | | | | | | | | | | 1 | | | |
| 13 | Time | | 1 | | | | | | | | | | | | | | | 1 | | |
| 14 | Sun direction | | * | 1 | | | | * | * | | | | | | | | | | | |
| 15 | Magnetic field dir. | | * | | 1 | | | * | * | | | | | | | | | | | |

The incidence matrix is the data source for the structural analysis and all subsequent steps depend on it. Whenever the incidence matrix changes (which means the system structure changed) the structural analysis has to be repeated.

## 5.3 Ranking Algorithm

After the incidence matrix is known the next step to generate residuals is to rank the constraints. The rank represents the amount of calculations required (or the amount of other constraints necessary) to eliminate all unknown states except one from the constraint equation (which allows solving the equation).

A basic ranking algorithm working on the incidence matrix is given in Figure 5-3.

The basic approach is to subsequently check all constraints for states not marked yet. In the beginning all known states are marked (these are states known e.g. through sensor measurements). Then all constraints with only one unmarked state can be solved and are assigned rank r = 0. The single unmarked state in these constraints is known afterwards and therefore marked in all other constraints. Because of these markings it might happen that some unranked constraints now have no unmarked states left. These constraints are marked with rank r = 1. This procedure is repeated with increasing r until all constraints are ranked.

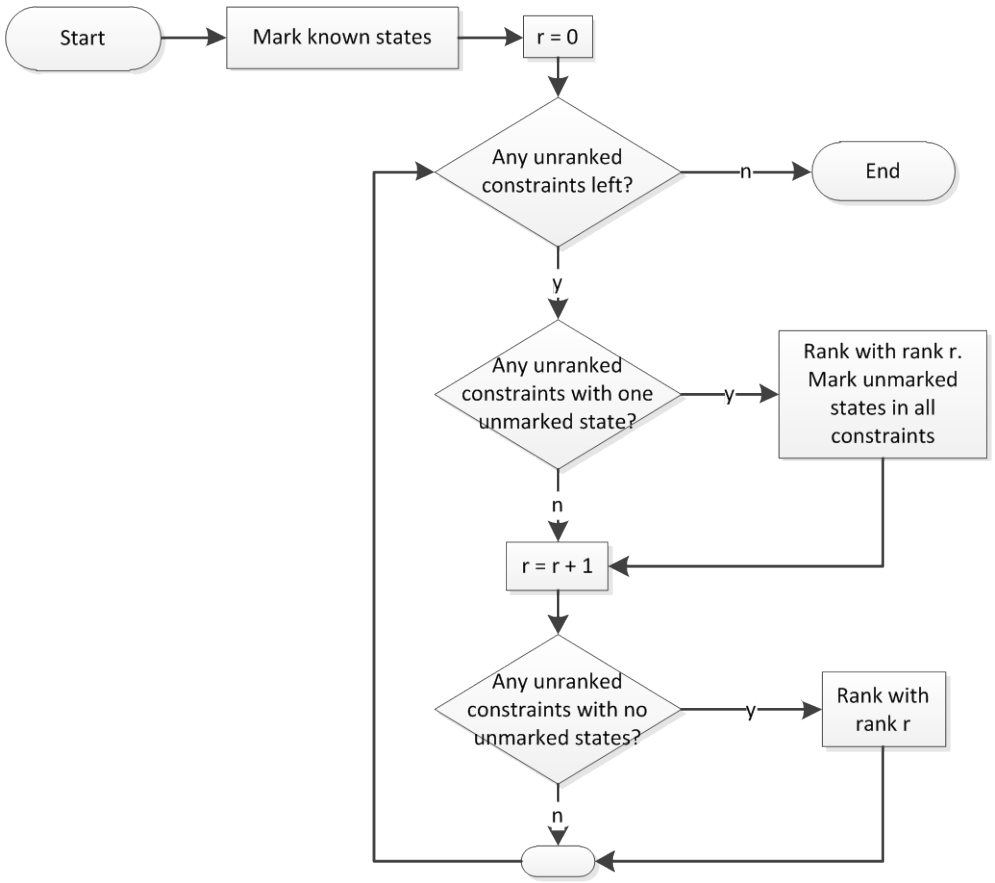


Figure 5-3: Basic ranking algorithm

In the following the ranking algorithm is applied to the exemplarily setup's incidence matrix. Step 1 is to mark all known states which is shown in Table 5-3, then r is set to zero.

Step 2 is to check for any constraints not ranked yet which have only one unmarked state. Table 5-4 shows that this is the case for constraints 1 to 7 and 10 to 13. The current rank r = 0 is assigned to them and all unmarked states used in these constraints are marked in all remaining constraints which can be seen in Table 5-5 (dark blue entries). In this case all unknown states are marked. Afterwards r is increased by one.

Table 5-3: Ranking algorithm step #1

| | | Unknown states | | | | | | | | Known states | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Constraint | Line of sight to client | Time | Sun direction | Magnetic field direction | Inertial rate | Inertial velocity | Inertial attitude | Inertial position | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 | Rank |
| 1 | Los FR Cam #1 | 1 | | | | | | | | 1 | | | | | | | | | | | |
| 2 | Los FR Cam #2 | 1 | | | | | | | | | 1 | | | | | | | | | | |
| 3 | Position GPS | | | | | | | | 1 | | | | | 1 | | | | | | | |
| 4 | Velocity GPS | | | | | | 1 | | | | | | 1 | | | | | | | | |
| 5 | Rate Gyro | | | | | 1 | | | | | | | | | 1 | | | | | | |
| 6 | Attitude star #1 | | | | | | | 1 | | | | | | | | | | | 1 | | |
| 7 | Attitude star #2 | | | | | | | 1 | | | | | | | | | | | | 1 | |
| 8 | Attitude derivative | | | | | 1 | | * | | | | | | | | | | | | | |
| 9 | Position derivative | | | | | | 1 | | * | | | | | | | | | | | | |
| 10 | CESS | | | 1 | | | | | | | | 1 | | | | | | | | | |
| 11 | Mag #1 | | | | 1 | | | | | | | | | | | 1 | | | | | |
| 12 | Mag #2 | | | | 1 | | | | | | | | | | | | 1 | | | | |
| 13 | Time | | 1 | | | | | | | | | | | | | | | 1 | | | |
| 14 | Sun direction | | * | 1 | | | | * | * | | | | | | | | | | | | |
| 15 | Magnetic field dir | | * | | 1 | | | * | * | | | | | | | | | | | | |

Table 5-4: Ranking algorithm step #2

| | | Unknown states | | | | | | | | Known states | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Constraint | Line of sight to client | Time | Sun direction | Magnetic field direction | Inertial rate | Inertial velocity | Inertial attitude | Inertial position | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 | Rank |
| 1 | Los FR Cam #1 | 1 | | | | | | | | 1 | | | | | | | | | | | 0 |
| 2 | Los FR Cam #2 | 1 | | | | | | | | | 1 | | | | | | | | | | 0 |
| 3 | Position GPS | | | | | | | | 1 | | | | | 1 | | | | | | | 0 |
| 4 | Velocity GPS | | | | | | 1 | | | | | | 1 | | | | | | | | 0 |
| 5 | Rate Gyro | | | | | 1 | | | | | | | | | 1 | | | | | | 0 |
| 6 | Attitude star #1 | | | | | | | 1 | | | | | | | | | | | 1 | | 0 |
| 7 | Attitude star #2 | | | | | | | 1 | | | | | | | | | | | | 1 | 0 |
| 8 | Attitude derivative | | | | | 1 | | * | | | | | | | | | | | | | |
| 9 | Position derivative | | | | | | 1 | | * | | | | | | | | | | | | |
| 10 | CESS | | | 1 | | | | | | | | 1 | | | | | | | | | 0 |
| 11 | Mag #1 | | | | 1 | | | | | | | | | | | 1 | | | | | 0 |
| 12 | Mag #2 | | | | 1 | | | | | | | | | | | | 1 | | | | 0 |
| 13 | Time | | 1 | | | | | | | | | | | | | | | 1 | | | 0 |
| 14 | Sun direction | | * | 1 | | | | * | * | | | | | | | | | | | | |
| 15 | Magnetic field dir. | | * | | 1 | | | * | * | | | | | | | | | | | | |

Next is to check for any unranked constraints with no unmarked states left. As can be seen in Table 5-5 this is the case for all remaining constraints (constraints 8, 9, 14, 15). The current rank r = 1 is assigned to them.

Now all constraints are ranked and the ranking process is finished.

As an example constraint 14 has rank 1 which means one step is required to calculate this constraint with only known states. Constraint 14 requires the unknown states time, sun direction, inertial attitude and inertial position to be evaluated. These unknown states can e.g. be determined by constraints 13, 10, 6 and 3 from known states but it requires one step to do this.

Table 5-5: Ranking algorithm step #3

| | | Unknown states | | | | | | | | Known states | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Constraint | Line of sight to client | Time | Sun direction | Magnetic field direction | Inertial rate | Inertial velocity | Inertial attitude | Inertial position | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 | Rank |
| 1 | Los FR Cam #1 | 1 | | | | | | | | 1 | | | | | | | | | | | 0 |
| 2 | Los FR Cam #2 | 1 | | | | | | | | | 1 | | | | | | | | | | 0 |
| 3 | Position GPS | | | | | | | | 1 | | | | | 1 | | | | | | | 0 |
| 4 | Velocity GPS | | | | | | 1 | | | | | | 1 | | | | | | | | 0 |
| 5 | Rate Gyro | | | | | 1 | | | | | | | | | 1 | | | | | | 0 |
| 6 | Attitude star #1 | | | | | | | 1 | | | | | | | | | | | 1 | | 0 |
| 7 | Attitude star #2 | | | | | | | 1 | | | | | | | | | | | | 1 | 0 |
| 8 | Attitude derivative | | | | | 1 | | * | | | | | | | | | | | | | 1 |
| 9 | Position derivative | | | | | | 1 | | * | | | | | | | | | | | | 1 |
| 10 | CESS | | | 1 | | | | | | | | 1 | | | | | | | | | 0 |
| 11 | Mag #1 | | | | 1 | | | | | | | | | | | 1 | | | | | 0 |
| 12 | Mag #2 | | | | 1 | | | | | | | | | | | | 1 | | | | 0 |
| 13 | Time | | 1 | | | | | | | | | | | | | | | 1 | | | 0 |
| 14 | Sun direction | | * | 1 | | | | * | * | | | | | | | | | | | | 1 |
| 15 | Magnetic field dir. | | * | | 1 | | | * | * | | | | | | | | | | | | 1 |

## 5.4 Matching

In terms of structural analysis a (optimal) matching on the structure graph defines the (fastest) way to calculate unknown states from known ones. If a constraint with unknown states has to be solved the matched constraints for each unknown state can be used to solve the constraint using only known states.

A valid matching matches each unknown state with a different constraint. That means each constraint can only be used in one matching. Also each unknown state is only matched once.

A complete matching with respect to the unknown states is a matching that is valid and that matches all unknown states.

If the matching is not complete it means that some of the unknown states cannot be computed and are therefore not observable.

There are several methods developed in graph theory to find a matching. The method used here is to use the ranks calculated in Section 4.2 to find a matching which is optimal in terms of computational steps required to reach the known states.

Each unknown state is matched with the lowest ranked constraint not used yet in a matching. If there are multiple equally ranked unmatched constraints available for a matching the first one (or a random one) is picked.

Application of this algorithm to the incidence matrix of the exemplarily setup results in a complete matching as shown in Table 5-6. In this case it was possible to use only rank 0 constraints for the complete matching. The matched constraint / state pairs are marked with a red border and the matched constraints are marked with a red background. It can be seen that for the complete matching of 8 unknown states 8 constraints are necessary (constraints 1, 3-6, 10, 11 and 13).

The most interesting result from this matching is that the 7 remaining, unmatched constraints (constraints 2, 7-9, 12, 14, 15) carry redundant information as they are not required to determine all unknown states. This information is exploited in Section 5.5.

Table 5-6: Complete optimal matching of the unknown states

| | | Unknown states | | | | | | | | Known states | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Constraint | Line of sight to client | Time | Sun direction | Magnetic field direction | Inertial rate | Inertial velocity | Inertial attitude | Inertial position | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 | Rank |
| 1 | Los FR Cam #1 | 1 | | | | | | | | 1 | | | | | | | | | | | 0 |
| 2 | Los FR Cam #2 | 1 | | | | | | | | | 1 | | | | | | | | | | 0 |
| 3 | Position GPS | | | | | | | | 1 | | | | | 1 | | | | | | | 0 |
| 4 | Velocity GPS | | | | | | 1 | | | | | | 1 | | | | | | | | 0 |
| 5 | Rate Gyro | | | | | 1 | | | | | | | | | 1 | | | | | | 0 |
| 6 | Attitude star #1 | | | | | | | 1 | | | | | | | | | | | 1 | | 0 |
| 7 | Attitude star #2 | | | | | | | 1 | | | | | | | | | | | | 1 | 0 |
| 8 | Attitude derivative | | | | | 1 | | * | | | | | | | | | | | | | 1 |
| 9 | Position derivative | | | | | | 1 | | * | | | | | | | | | | | | 1 |
| 10 | CESS | | | 1 | | | | | | | | 1 | | | | | | | | | 0 |
| 11 | Mag #1 | | | | 1 | | | | | | | | | | | 1 | | | | | 0 |
| 12 | Mag #2 | | | | 1 | | | | | | | | | | | | 1 | | | | 0 |
| 13 | Time | | 1 | | | | | | | | | | | | | | | 1 | | | 0 |
| 14 | Sun direction | | * | 1 | | | | * | * | | | | | | | | | | | | 1 |
| 15 | Magnetic field dir. | | * | | 1 | | | * | * | | | | | | | | | | | | 1 |

## 5.5 Residual Generation

As mentioned above, the unmatched constraints represent the redundant information available in the system.

The residual generation process is now straight-forward: each unmatched constraint is traced back to the known states and yields one residual. This is done by replacing all unknown states with the matched constraints from the matching derived above until only known states are left.

This results in only structural information about the residuals, e.g. residual x depends on known states a, b and c. For evaluation of the residual it is necessary to use the actual formulas of the constraints which are shown exemplary for one of the residuals later.

The numbering of the 7 residuals can be found in Table 5-7.

Table 5-7: Base constraints for residuals.

| | | Unknown states | | | | | | | | Known states | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Constraint | Line of sight to client | Time | Sun direction | Magnetic field direction | Inertial rate | Inertial velocity | Inertial attitude | Inertial position | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 | Residual |
| 1 | Los FR Cam #1 | 1 | | | | | | | | 1 | | | | | | | | | | | |
| 2 | Los FR Cam #2 | 1 | | | | | | | | | 1 | | | | | | | | | | 1 |
| 3 | Position GPS | | | | | | | | 1 | | | | | 1 | | | | | | | |
| 4 | Velocity GPS | | | | | | 1 | | | | | | 1 | | | | | | | | |
| 5 | Rate Gyro | | | | | 1 | | | | | | | | | 1 | | | | | | |
| 6 | Attitude star #1 | | | | | | | 1 | | | | | | | | | | | 1 | | |
| 7 | Attitude star #2 | | | | | | | 1 | | | | | | | | | | | | 1 | 2 |
| 8 | Attitude derivative | | | | | 1 | | * | | | | | | | | | | | | | 3 |
| 9 | Position derivative | | | | | | 1 | | * | | | | | | | | | | | | 4 |
| 10 | CESS | | | 1 | | | | | | | | 1 | | | | | | | | | |
| 11 | Mag #1 | | | | 1 | | | | | | | | | | | 1 | | | | | |
| 12 | Mag #2 | | | | 1 | | | | | | | | | | | | 1 | | | | 5 |
| 13 | Time | | 1 | | | | | | | | | | | | | | | 1 | | | |
| 14 | Sun direction | | * | 1 | | | | * | * | | | | | | | | | | | | 6 |
| 15 | Magnetic field dir. | | * | | 1 | | | * | * | | | | | | | | | | | | 7 |

As an example residual #7 which is based on constraint #15 is derived here. Table 5-8 lists dependency of constraint #15 from time, magnetic field direction, inertial attitude and inertial position. The unknown states are matched as follows:

- Time: Matched by constraint #13 from the measurement of GPS time
- Magnetic field direction: Matched by constraint #11 from magnetometer #1
- Inertial attitude: Matched by constraint #6 from measurement of star tracker #1
- Inertial position: Matched by constraint #3 from measurement of GPS position

Replacing the unknown states by these constraints results in a residual depending on only known states (namely GPS time, GPS position, magnetometer #1 and star tracker #1) as shown in Table 5-9.

To get the actual equation for the residual it is necessary to evaluate the equations of the constraints involved.

1. GPS inertial position measurement $r_{\mathrm{SS}} = r_{\mathrm{GPS}}$
2. Star tracker #1 inertial orientation measurement $q_{\mathrm{SS}} = q_{\mathrm{Star1}}$
3. Magnetometer #1 magnetic field direction measurement $m_{\mathrm{SS}} = m_{\mathrm{Mag1}}$
4. GPS time measurement $t_{\mathrm{SS}} = t_{\mathrm{GPS}}$
5. Magnetic field model $m_{\mathrm{SS}} = T_{SS,I}\left(q_{\mathrm{SS}}\right) \cdot m\left(r_{\mathrm{SS}}, t_{\mathrm{SS}}\right)$

Substituting the unknown states in constraint 5) by constraints 1) to 4) yields the residual

$$R_7 = m_{\mathrm{Mag1}} - T_{SS,I}\left(q_{\mathrm{Star1}}\right) \cdot m\left(r_{\mathrm{GPS}}, t_{\mathrm{GPS}}\right)$$

which should be zero (neglecting noise) when no faults are present. This residual evaluates the magnetic field model with the data measured by GPS and star tracker and compares it to the magnet field direction measured by the magnetometer – obviously the information from both sources should be the same.

Repeating this procedure for each of the remaining 6 residuals gives to the following result (the subtractions have to be seen symbolic, e.g. when evaluating residual #2 it is the multiplication of $q_{Star1}$ with the inverse quaternion of $q_{Star2}$)

$$R_1 = p_{\mathrm{CAMFR1}} - p_{\mathrm{CAMFR2}}$$
$$R_2 = q_{\mathrm{Star1}} - q_{\mathrm{Star2}}$$
$$R_3 = \omega_{\mathrm{Gyro1}} - \frac{d}{dt} q_{\mathrm{Star1}}$$
$$R_4 = r_{\mathrm{GPS}} - v_{\mathrm{GPS}}$$
$$R_5 = m_{\mathrm{Mag1}} - m_{\mathrm{Mag2}}$$
$$R_6 = s_{\mathrm{CESS}} - \mathrm{T}_{SS,I}\left(q_{\mathrm{Star1}}\right) \cdot s\left(r_{\mathrm{GPS}}, t_{\mathrm{GPS}}\right)$$
$$R_7 = m_{\mathrm{Mag1}} - T_{SS,I}\left(q_{\mathrm{Star1}}\right) \cdot m\left(r_{\mathrm{GPS}}, t_{\mathrm{GPS}}\right)$$

With the knowledge of the known states used in each residual it is possible to make a clear statement about the possibility to detect and localize faults in the individual known states, which is described in detail in section 5.6.

Table 5-8: Residual #7 generation step #1

| | | Unknown states | | | | | | | | Known states | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Constraint | Line of sight to client | Time | Sun direction | Magnetic field direction | Inertial rate | Inertial velocity | Inertial attitude | Inertial position | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 | Residual |
| 1 | Los FR Cam #1 | 1 | | | | | | | | 1 | | | | | | | | | | | |
| 2 | Los FR Cam #2 | 1 | | | | | | | | | 1 | | | | | | | | | | 1 |
| 3 | Position GPS | | | | | | | | 1 | | | | | 1 | | | | | | | |
| 4 | Velocity GPS | | | | | | 1 | | | | | | 1 | | | | | | | | |
| 5 | Rate Gyro | | | | | 1 | | | | | | | | | 1 | | | | | | |
| 6 | Attitude star #1 | | | | | | | 1 | | | | | | | | | | | 1 | | |
| 7 | Attitude star #2 | | | | | | | 1 | | | | | | | | | | | | 1 | 2 |
| 8 | Attitude derivative | | | | | 1 | | * | | | | | | | | | | | | | 3 |
| 9 | Position derivative | | | | | | 1 | | * | | | | | | | | | | | | 4 |
| 10 | CESS | | | 1 | | | | | | | | 1 | | | | | | | | | |
| 11 | Mag #1 | | | | 1 | | | | | | | | | | | 1 | | | | | |
| 12 | Mag #2 | | | | 1 | | | | | | | | | | | | 1 | | | | 5 |
| 13 | Time | | 1 | | | | | | | | | | | | | | | 1 | | | |
| 14 | Sun direction | | * | 1 | | | | * | * | | | | | | | | | | | | 6 |
| 15 | Magnetic field dir. | | * | | 1 | | | * | * | | | | | | | | | | | | 7 |

Table 5-9: Residual #7 generation step #2

| | | Unknown states | | | | | | | | Known states | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | Constraint | Line of sight to client | Time | Sun direction | Magnetic field direction | Inertial rate | Inertial velocity | Inertial attitude | Inertial position | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 | Residual |
| 1 | Los FR Cam #1 | 1 | | | | | | | | 1 | | | | | | | | | | | |
| 2 | Los FR Cam #2 | 1 | | | | | | | | | 1 | | | | | | | | | | 1 |
| 3 | Position GPS | | | | | | | | 1 | | | | | 1 | | | | | | | |
| 4 | Velocity GPS | | | | | | 1 | | | | | | 1 | | | | | | | | |
| 5 | Rate Gyro | | | | | 1 | | | | | | | | | 1 | | | | | | |
| 6 | Attitude star #1 | | | | | | | 1 | | | | | | | | | | | 1 | | |
| 7 | Attitude star #2 | | | | | | | 1 | | | | | | | | | | | | 1 | 2 |
| 8 | Attitude derivative | | | | | 1 | | * | | | | | | | | | | | | | 3 |
| 9 | Position derivative | | | | | | 1 | | * | | | | | | | | | | | | 4 |
| 10 | CESS | | | 1 | | | | | | | | 1 | | | | | | | | | |
| 11 | Mag #1 | | | | 1 | | | | | | | | | | | 1 | | | | | |
| 12 | Mag #2 | | | | 1 | | | | | | | | | | | | 1 | | | | 5 |
| 13 | Time | | 1 | | | | | | | | | | | | | | | 1 | | | |
| 14 | Sun direction | | * | 1 | | | | * | * | | | | | | | | | | | | 6 |
| 15 | Magnetic field dir. | | * | | 1 | | | * | * | | | | | | | | | | | | 7 |

## 5.6 Fault Signatures

A fault is defined as the deviation of one of the known states from its nominal (and correct) value. If that happens for exactly one of the known states, all residuals using that state will deviate from zero (the residual is activated). To prevent residual activation due to normal noise levels some sort of filtering might be necessary.

Listing the residuals as the rows and the known states as the columns of a matrix and marking each cell where the known state is used in the residual results in Table 5-10. The columns of this table are the fault signatures of the corresponding known states (which are the sensor measurements in the exemplarily case).

Table 5-10: Fault signatures for exemplarily setup

| Residual | Base constraint | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Los FR Cam #2 | ■ | ■ | | | | | | | | | |
| 2 | Attitude star #2 | | | | | | | | | | ■ | ■ |
| 3 | Attitude derivative | | | | | | ■ | | | | ■ | |
| 4 | Position derivative | | | | ■ | ■ | | | | | | |
| 5 | Mag #2 | | | | | | | ■ | ■ | | | |
| 6 | Sun direction | | | ■ | | ■ | | | | ■ | ■ | |
| 7 | Magnetic field direction | | | | | ■ | | ■ | | ■ | ■ | |

The first important result that can be derived from this matrix is that for all states with at least one marked cell (that means non-empty columns) it is possible to detect faults. As can be seen in Table 5-10 it is theoretically possible (due to the system structure) to detect faults in all of the states for the exemplarily setup.

The second important result is the possibility to tell which faults can be localized. Each fault with a fault signature (column) that is different from all other fault signatures (columns) can be unambiguously distinguished from other faults. That also means that faults which share a fault signature cannot be distinguished. To automate the task of determining the possibility of localization each residual is assigned a value of $2^{(\text{residualnumber}-1)}$.

Now for each fault signature the sum of residual values for marked residuals is calculated. Each fault with a fault signature value different from all other values is distinguishable while faults sharing the fault signature value are not.



Doc.No.: GAFE-UM-D7.5a
Issue: 2.0
Date: 13.06.2018

Table 5-11: Classification of fault signatures for exemplarily setup

| Residual | Base constraint | Line of sight far-range camera #1 | Line of sight far-range camera #2 | Sun direction CESS | Inertial velocity GPS | Inertial position GPS | Inertial rate gyro | Magnetic field direction mag #1 | Magnetic field direction mag #2 | Time GPS | Inertial attitude startracker #1 | Inertial attitude startracker #2 | Residual Value | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Los FR Cam #2 | | | | | | | | | | | | 1 | 2^0 |
| 2 | Attitude star #2 | | | | | | | | | | | | 2 | 2^1 |
| 3 | Attitude derivative | | | | | | | | | | | | 4 | 2^2 |
| 4 | Position derivative | | | | | | | | | | | | 8 | 2^3 |
| 5 | Mag #2 | | | | | | | | | | | | 16 | 2^4 |
| 6 | Sun direction | | | | | | | | | | | | 32 | 2^5 |
| 7 | Magnetic field direction | | | | | | | | | | | | 64 | 2^6 |
| | Fault Signature Value: | 1 | 1 | 32 | 8 | 104 | 4 | 80 | 16 | 96 | 102 | 2 | | |

Table 5-11 shows the result for the exemplarily setup: All faults except faults in the far range cameras are localizable as they have different fault signature values. The two far range cameras share the same fault signature value (1) and therefore it is not possible to tell which far range camera is faulty if a fault occurs in one of them.

When more than one fault has to be distinguished it is necessary that the fault signatures (the columns) are linearly independent from each other. That means that each combination of faults has an unambiguously distinguishable value. For the exemplarily setup this is obviously not the case as the matrix has more columns than rows. Even when reducing the system by removing the far range camera subsystem the number of columns is higher that the number of rows.

# 6 Appendix B: FDIR Related Analysis Methods

## 6.1 Failure Modes, Effects and Criticality Analysis (FMECA)

FMECA shows the failure modes, effects and criticalities of individual failure modes, generally in matrix form. This is a bottom-up technique and usually used late in the development process, after the components are selected. Nonetheless it might be possible to make a preliminary FMECA based on an early design.

The Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects, and Criticality Analysis (FMECA) are performed to systematically identify potential failures in products or processes and to assess their effects in order to define mitigation actions.

The failure modes identified through the Failure Mode and Effect Analysis (FMEA) are classified according to the severity of their consequences. The Failure Mode, Effects, and Criticality Analysis (FMECA) is an extension of FMEA, in which the failure modes are classified according to their criticality, i.e. the combined measure of the severity of a failure mode and its probability of occurrence.

The FME(C)A is basically a bottom-up analysis and it is not adapted to assess combination of failures. It is an effective tool in the decision making process, provided it is a timely and iterative activity. Late implementation or restricted application of the FMEA/FMECA dramatically limits its use as an active tool for improving the design or process.

There are different levels of FME(C)A:

- Functional FME(C)A: the functions, rather than the items used in their implementation, are analysed
- Hardware FME(C)A: the hardware used in the implementation of the product functions is analysed
- Process FMECA: the processes are analysed, including the effects of their potential failures (processes such as manufacturing, assembling and integration, pre-launch operations)

Figure 6-1 shows an example of an FMECA sheet for an AOCS level FMECA.

| Ident. No. | Item / Block | Function Description | Mission Phase / Operational Mode | Assumed Failure Mode / Cause | Occurence | Failure Effects on Equipment / Subsystem / System | Severity | Failure Detection / Observable Symptoms<br>Sensor built-in<br>Onboard FDI software<br>Not detectable | Detection | RPN / Risk Priority Number | Compensation / Prevention Methods | Remarks / Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| STRH01 | Star Tracker head | Supply camera image | All | Blinded (earth / sun in field of view) | 10 | No image -> No attitude estimation in electronics -> Attitude Filter has no update -> Drifting attitude estimate -> Loss of target, power, communication -> Collision risk | 10 | Detection in Star Tracker electronics | 1 | 100 | Use other head pointing in other direction | Visibility analysis for startracker heads (no sun, earth, moon, client, etc), nominal case |
| STRH02 | Star Tracker head | Supply camera image | All | Constant image | 2 | Constant image -> Constant attitude estimation in electronics -> Attitude Filter has constant attitude update -> Constant attitude estimate -> Loss of target, power, communication -> Collision risk | 10 | Detection in Star Tracker electronics | 1 | 20 | Use other head | |
| STRH03 | Star Tracker head | Supply camera image | All | Restart (e.g. due to heat problem or radiation) | 2 | Temporarily no image -> No attitude estimation in electronics -> Attitude Filter has no update -> Short time drifting attitude estimate -> Temporarily small attitude estimate error | 5 | Detection in Star Tracker electronics | 1 | 10 | Wait / Use other head | Restart time? |
| | Star | | | | | No image -> No attitude estimation in electronics -> | | | | | | |

Figure 6-1: Example FMECA sheet

A list of available FME(C)A software packages can be found in [RD-8].

## 6.2 Fault-Tree Analysis (FTA)

FTA is a top down approach to display the combinations of failures that can result in the main system failure of interest. Identification/assessment of risk is derived by first identifying faults/hazards.

The process is basically:

- A feared event is defined
- The event is resolved into its immediate causes
- This resolution of events continues until basic causes are identified
- A logical diagram called a fault tree is constructed showing the logical event relationships

FTA is a deductive analysis approach for resolving an undesired event into its causes. FTA is a backward looking analysis, looking backward at the causes of a given event. Specific stepwise logic is used in the process and specific logic symbols are used to illustrate the event relationships. A logic diagram is constructed showing the event relationships.

Goals of the FTA are e.g.:

- Exhaustively identify the causes of a failure
- Identify weaknesses in a system
- Assess a proposed design for its reliability or safety
- Quantify the failure probability and contributors

The basic structure of a fault tree is shown in Figure 6-2:

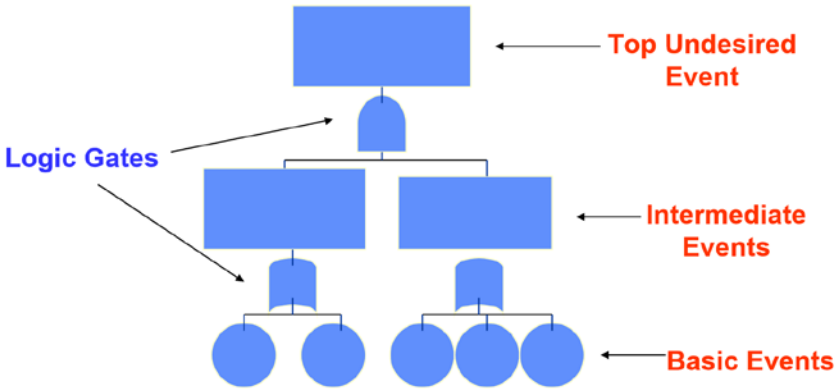


Figure 6-2: Basic Fault Tree Structure

Software packages for FTA are e.g. Open FTA, BlockSim and FaultTree+.

*Assessment: The FTA is one of the standard tools for FDIR engineers. It is very useful to discover failure root causes and weaknesses of a system and display fault event relationships. The resulting undesired / feared event probabilites can be used to drive the FDIR design process as they indicate where FDIR actions are requried. It should be used during the FDIR engineering process.*

# 7 Appendix C: Abbreviations, Terms & Definitions

## 7.1 List of Abbreviations

| Abbreviations | |
|---|---|
| **A** | |
| ACC | Accelerometer |
| ACQ | Acquisition Mode |
| ACT | Attitude Control Thruster |
| AD | Applicable Document |
| AFDIR | Advanced FDIR |
| AH | Attitude Hold |
| AHM | Attitude Hold Mode |
| AIT | Assembly, Integration, Test |
| ALGO | Algorithm |
| ALI | Advanced Land Imager |
| ALS | Alenia Spazio |
| AOC | Attitude & Orbit Control |
| AOCS | Attitude and Orbit Control System |
| AOS | Acquisition of Signal |
| APID | Application Process ID |
| APM | Antenna Pointing Mechanism |
| ARR | Analytic Redundancy Relation |
| ASM | Acquisition & Safe Mode |
| ASOS | Advanced Smart Observation Satellite |
| **B** | |
| BIT | Built-in Test |
| BN | Bayesian Network |
| BS | Blocking Surveillance |
| BSL | Back slew |
| **C** | |
| CA | Corrective Action |
| CAM | Camera |
| CBH | Catbed Heater |
| CDHS | Central Data Handling System |
| CDMS | Central Data Management System |
| CDMU | Central Data Management Unit |
| CDR | Critical Design Review |
| CESS | Coarse Earth & Sun Sensor |
| **K** | |
| **L** | |
| LCL | Latch-Current Limiter |
| LCT | Laser Communication Terminal |
| LIDAR | Light Detection and Ranging |
| LoS | Line of Sight |
| LPF | Livingstone PathFinder |
| LPV | Linear Parameter Varying |
| LRI | Laser Ranging Instrument |
| LTI | Linear Time Invariant |
| **M** | |
| MA | Mission assurance |
| MADM | Multi attribute decision making |
| MAG | Magnetometer |
| MBD | Model Based Diagnosis |
| MC | Monte-Carlo |
| MCA | Monte-Carlo Analysis |
| MDT | Maintenance Downtime |
| MEO | Medium Earth Orbit |
| MGSE | Mechanical Ground Support Equipment |
| MI | Mode identification |
| MIMU | Miniaturized Inertial Measurement Unit |
| MLR | Marginalized Likelihood Ratio |
| MMFU | Mass Memory Formation Unit |
| MO | Mars Observer |
| MOIS | Manufacturing and Operations Information System |
| MOS | Mission Operations System |
| MPL | Mars Polar Lander |
| MPPT | Maximum Power Point Tracker |
| MR | Mode reconfiguration |
| MRO | Mars Reconnaissance Orbiter |
| MSI | Multi-Spectral Instrument |
| MSL | Mars Science Lab |
| MTBM | Mean Time Between |

| | |
|---|---|
| CFI | Costumer Furnished Item |
| CGPS | Cold Gas Propulsion System |
| CGS | Cold Gas System |
| CICPM | CESS/IMU Coarse Pointing Mode |
| CMM | Constellation Maintenance Mode |
| CN | Causal Network |
| COM/CoM | Communication or Center of Mass |
| CP | Control Procedure |
| CPM | Coarse Pointing Mode |
| CPU | Central Processing Unit |
| CT | Correlation Test |
| CUSUM | Cumulative Sum |
| **D** | |
| DAS | Data Acquisition Status |
| DB | Data Base |
| DBN | Dynamic Bayesian Network |
| DD | Dependence Diagram |
| DDN | Dynamic Decision Network |
| DEP | Deployment |
| DFT | Dynamic Fault-Tree |
| DHS | Data Handling System |
| DS | Deep Space |
| DSS | Digital Sun Sensor |
| DTU | Technical University of Denmark |
| **E** | |
| EA | Earth Acquisition |
| ECEF | Earth Centered Earth Fixed |
| ECSS | European Cooperation for Space Standardization |
| ECT | Equipment Configuration Table |
| EDFT | Extended Dynamic Fault Tree |
| EDL | Entry Decent Landing |
| EDM | Entry and Descent Module |
| EES | Extended AOCS Equipment Set |
| EGSE | Electrical Ground Support Equipment |
| EML | Embedded MATLAB |
| | Maintenance |
| MTQ | Magnettorquer |
| **N** | |
| NaN | Not a Number |
| NES | Nominal AOCS Equipment Set |
| NOM | Normal Mode |
| NP | Non-deterministic polynomial-time |
| **O** | |
| OBC | On-board Computer |
| OBDH | On-board Data Handling |
| OBMP | On-board Macro Procedure |
| OBSW | On-board Software |
| OCP | On-board Control Procedure |
| OGSE | Optical Ground Support Equipment |
| OLS | Off-Line Surveillance |
| OOL | Out Off Limit |
| OoM | Order of magnitude |
| OOP | On-board Orbit Propagator |
| OoR | Out-of-Range |
| OP | Operational |
| **P** | |
| PCDU | Power Conditioning and Distribution Unit |
| PDR | Preliminary Design Review |
| PITEX | Propulsion Integrated Vehicle Health Management (IVHM) Technology Experiment |
| PM | Processor Module (of OBC) |
| POC | Point of contact |
| PRA | Probabilistic risk assessment |
| PRID | Process ID |
| PRNG | Pseudo-Random Number Generator |
| PUS | Packet Utilization Standard |
| PWR | Power |
| **Q** | |
| **R** | |
| RAMS | Reliability, Availability, Maintainability, and Safety |
| RBD | Reliability Block Diagram |
| RCS | Reaction Control System |

| | |
|---|---|
| | Language |
| EP | Electric Propulsion |
| ES | Earth Sensor |
| ESOC | European Space Operations Centre |
| ESTEC | European Space Research and Technology Centre |
| ETA | Event Tree Analysis |
| EWMA | Exponentially weighted moving averages |
| **F** | |
| FAR | Flight Acceptance Review |
| FCL | Flight control laws |
| FCP | Flight Control Procedure |
| FD | Fault Detection |
| FDD | Fault Detection and Diagnosis |
| FDI | Fault Detection and Isolation |
| FDIR | Fault Detection, Isolation and Recovery |
| FDV | Fill Drain Valve |
| FEPP | Failure Effect Propagation Path |
| FES | Functional Engineering Simulator |
| FF | Formation Flight |
| FFT | Fast Fourier Transform |
| FGM | Field Gate Magnetometer |
| FIR | Fuzzy Inductive Reasoning |
| FM | Fault Management |
| FME(C)A | Failure Mode, Effects and (Criticality) Analysis |
| FOM | Flight Operation Manual |
| FOS | Flight Operation System |
| FoV | Field of View |
| FP | Fault Protection or Fine Pointing |
| FPM | Fine Pointing Mode |
| FR | Far Range or Failure Recovery |
| FRA | Failure Response Analysis |
| FT | Fault Tree |
| FTA | Fault Tree Analysis |
| FTC | Fault tolerant control |
| **G** | |
| GAFE | GNC/AOCS FDIR Engineering Framework |
| GEM | Generic Equipment Model |
| GEO | Geostationary Orbit |
| | (Propulsion System) |
| RD | Rate Damping Mode |
| RD | Reference Documents |
| RDM | Rate Damping Mode |
| RMU | Rate Measurement Unit |
| RNS | Relative Navigation Sensor |
| RSPF | Risk Sensitive Particle Filter |
| RTI | Real-time interface |
| RU | Remote Unit |
| RvD | Rendezvous and Docking |
| RW | Reaction Wheel |
| RWA | Reaction Wheel Assembly |
| **S** | |
| SA | Structural Analysis |
| SADM | Solar Array Driving Mechanism |
| SAR | Synthetic Aperture Radar |
| SC | Spacecraft |
| SCL | Spacecraft Command Language |
| SCOE | Special Check-Out Equipment |
| SCV | Spacecraft Configuration Vector |
| SDP | System Data Pool |
| SE | System Engineering |
| SEM | Specific Equipment Model |
| SEU | Single Event Upset |
| SFM | Safe Mode |
| SFT | System Functional Test |
| SGM | Safeguard Memory |
| SPF | Space Power Facility |
| SS | Sun Sensor |
| SS | Sun Sensor |
| SSUM | Space Segment User Manual |
| STAB | Stabilization Mode |
| STBY | Stand-By |
| STR | Star Tracker |
| STRE | Star Tracker Electronics |
| STRS | Star Tracker System |
| SVM | Support vector machine |
| SVN | Subversion (Version Control |

| | |
|---|---|
| | |
| GLR | Generalized Likelihood Ratio |
| GLT | Generalized Likelihood Test |
| GNC | Guidance, Navigation & Control |
| GNSR | GNSS Receiver |
| GNSS | Global Navigation Satellite System |
| GOCE | Gravity Field and Steady-State Ocean Circulation Explorer |
| GPS | Global Positioning System |
| GPSR | GPS Receiver |
| GUI | Graphical User Interface |
| **H** | |
| HA | Hazard analysis |
| HIL | Hardware in the loop |
| HITL | Hardware in the Loop |
| HK | Housekeeping |
| HPCM | High Priority Command |
| HPLV | High Pressure Latch Valve |
| HW | Hardware |
| **I** | |
| IAM | Initial Acquisition Mode |
| IC | Integrated Circuit |
| ID | Identifier |
| IMU | Inertial Measurement Unit |
| ISL | Inter Satellite Link |
| ISS | International Space Station |
| **J** | |
| JPL | Jet Propulsion Lab |
| JT | Junction tree |

| | |
|---|---|
| | Concept) |
| SW | Software |
| **T** | |
| TAFF | TanDEM Autonomous Formation Flying |
| TAI | "Temps Atomique International" / International Atomic Time |
| TBC | To be confirmed |
| TBD | To be defined |
| TC | Telecommand |
| TCS | Thermal Control System |
| TDX | TanDEM-X |
| TFPG | Timed Failure Propagation Graph |
| TGO | Trace Gas Orbiter |
| THR | Propulsion System/Thruster |
| TMMM | Telemetry and Mass Memory Module |
| TPM | Thruster Pointing Mechanism |
| TSX | TerraSAR-X |
| TTC | Telemetry, Tracking and Command |
| **U** | |
| UHT | Unit Health Table |
| UIO | Unknown input observer |
| USBL | Usable |
| UUV | Unit Unavailability Vector |
| **V** | |
| VRPF | Variable Resolution Particle Filter |
| **W** | |
| **X** | |
| **Y** | |
| **Z** | |

## 7.2 List of Terms & Definitions

| Term | Description | Category |
|---|---|---|
| **A** | | |
| Analytic Redundancy Relation | A concept to determine consistency between not directly comparable quantities by means of mathematical/physical models (e.g. for the spacecraft attitude measured by star tracker and spacecraft rate measured by rate measurement unit via differentiation). | FDIR |
| AOCS Main-Mode | In general AOCS main modes serve different purposes (e.g. instrument operation, orbit maintenance, safeguarding) and usually require different AOCS equipment to be operated. AOCS main modes are often subdivide into *AOCS Sub-Modes*. | AOCS |
| AOCS Sub-Mode | Often AOCS Main Mode consists of several AOCS sub-modes, which break the different aspects of the main mode down into a sequence of more elementary tasks (e.g. rate damping, sun acquisition, earth acquisition for an acquisition and safe mode). Different sub-modes of one main mode can use different software functions (algorithms), but the active equipment set is the same. | AOCS |
| **B** | | |
| **C** | | |
| Component | A part of a module. | Simulator |
| Cold Redundancy | See *Redundancy* | Fault Management |
| **D** | | |
| Detectability Anaylsis | The analysis if a set of faults is in principle detectable (with the available information). | |
| Device | See *Unit.* | AOCS |
| **E** | | |
| Equipment | An entity summarizing all sensor or actuator units of the same type. See also *unit.*All types of different equipment together is called equipment set (e.g. nominal *equipment set* for AOCS nominal mode) | AOCS |
| Equipment Set | All types of different (AOCS) equipment together is called equipment set (e.g. the nominal *equipment set* for AOCS nominal mode consists of 3 STR, 2 GPS and 4 RWs). | AOCS |
| Error | Deviation between a measured or computed value (of an output variable) and the true, specified, or theoretically correct value. | FDIR |
| **F** | | |
| Fail Operational | A failure is autonomously detected and resolved onboard such that the scheduled operation of the concerned functionality is continued without the need for ground intervention. Fail Operational is the opposite concept to *Fail Safe*. | Fault Management |

| | | |
|---|---|---|
| Fail Safe | A failure is autonomously detected and resolved onboard such that the scheduled operation of the concerned functionality is terminated and the affected subsystem, payload or spacecraft is switched into a safe state (i.e. one in which the major functions are preserved, see Safe Mode) until ground intervenes to restore scheduled operations. Fail Safe is the opposite concept to Fail Operational. | Fault Management |
| Failure | Permanent interruption of a systems ability to perform a required function under specified operating conditions. | Fault Management |
| Failure | The unacceptable performance of an intended function. | |
| Failure Avoidance | Predict that a failure will occur in the future and take action to prevent it from happening, generally through repair, replacement, or operational changes that reduce the failure's probability or delay its occurrence. | Fault Management |
| Failure Prevention | In failure prevention, actions are taken to ensure that failures will not occur. | Fault Management |
| Fault | Undesired change in the system that tends to degrade overall system performance, although it may not represent the failure of physical components. | Fault Management |
| Fault Accommodation | The action of changing the control law in response to fault, without switching off any system component. In fault accommodation, faulty components are still kept in operation thanks to an adapted control law. | FDIR |
| Fault Avoidance | Passive prevention of faults by a less fault-prone design, e.g. higher margins, stricter quality assurance processes, higher quality parts. | Fault Management |
| Fault Containment | To prevent a fault from causing further faults. | FDIR |
| Fault Detection | To provide information on the presence or absence of faults in the functional units of the process, which lead to undesired or intolerable behaviour of the whole system. | FDIR |
| Fault Diagnosis | To determine kind, size, location, and time of occurrence of a fault. Fault diagnosis includes fault detection, isolation and estimation. | FDIR |
| Fault Estimation | To determine a model of the faulty system. | FDIR |
| Fault Identification | To determine the size and time-variant behaviour of a fault. | FDIR |
| Fault Isolation | To determine the type and location of a fault once it is known that a fault has occurred. | FDIR |
| Fault Management | The engineering discipline that encompasses practices for enabling operational systems to contain, prevent, detect, isolate, diagnose, respond to, and recover from conditions that may interfere with nominal mission operations. | Fault Management |
| Fault Management Strategy | How a fault is considered in the design, i.e. either via fault prevention or fault tolerance. | Fault Management |
| Fault Masking | Allow a fault to produce a lower level failure, but mask its effects, e.g. by majority voting, so that it does not affect the higher level system function. | Fault Management |
| Fault Recovery | Fault accommodation or system reconfiguration. An action | FDIR |

| | | |
|---|---|---|
| | taken to restore functions necessary to achieve existing or redefined system goals after a failure. | |
| Fault Tolerance | The ability to perform a function in the presence of any of a specified number of coincident and independent failure causes of specified types. In failure tolerance, failures are allowed to occur, but their effects are mitigated or accepted. | Fault Management |
| FDI | Fault Detection and Isolation. | FDIR |
| FDIR | Fault Detection, Isolation and Recovery. | FDIR |
| FDIR Architecture | Combination of FDIR functions to HW/SW functional chains making up a S/C system specific FDIR structure. | FDIR System |
| FDIR Design | FDIR engineering until the Critical Design Review (CDR), i.e. specification, definition, etc. | FDIR Engineering |
| FDIR Development | FDIR engineering after the Critical Design Review (CDR), i.e. implementation, qualification, testing, etc. | FDIR Engineering |
| FDIR Engineering | Any engineering activity related to FDIR design and development. | FDIR Engineering |
| FDIR Hierarchical levels | Allocation of FDIR responsibility to a hierarchical structure containing S/C HW and SW. | FDIR System |
| FDIR Mechanism | Functional chain and its realization for a distinct fault detection, isolation and recovery case, excluding monitor generation. | FDIR System |
| FDIR Model-Based Design | Use of models to represent FDIR system in the design process. | FDIR Engineering |
| Framework | Software tools that support the engineering process. | Engineering |
| **G** | | |
| GNC | Guidance, Navigation & Control. In the scope of the study used equivalently to the term AOCS. | AOCS |
| Goal Change | Allow a failure to compromise the system function, and respond by changing the system's goals to new, usually degraded (secondary) goals that can be achieved. | Fault Management |
| **H** | | |
| Hot Redundancy | See Redundancy | Fault Management |
| **I** | | |
| Isolability Anaylsis | The analysis if each fault within a set of faults can be distinguished unambiguously from all others. | |
| **J** | | |
| **K** | | |
| **L** | | |
| **M** | | |
| Method | Techniques and theoretical elements with empirical and measurable evidence to find a solution to a practical problem definition. | Engineering |
| Methodology | Methodology is not the same as method. It is the | Engineering |

| | | |
|---|---|---|
| | systematic approach and strategy of applying a set of methods in the design and development of a system, product, etc. | |
| Model-based Fault Detection and Isolation (FDI) | Use of models inside FDI functionality to identify faults and generate monitors (e.g. observers to generate residuals). | FDIR System |
| Module | An entity with well-defined interfaces which is composed of compnents. | Simulator |
| Monitor | Measurements that are conditioned and processed to indicate a fault or even already represent the failure state of a system. | FDIR System |
| **N** | | |
| **O** | | |
| Observable (parameter) | Any kind of value, parameter, status information or derived quanitity visible to the FDIR. | FDIR |
| **P** | | |
| Process | A process implements the methodology (with its methods). It defines the methodological design and development flow with the required inputs and outputs. In this context it provides practical and systematic step-by-step instructions and guidelines of how to apply the methodology to obtain a coherent system design. | Engineering |
| **Q** | | |
| **R** | | |
| Residual | The output of monitor generator; it represents the deviation of a model-based computation result from e.g. an expected value/behavior or a measured quantity. | FDIR System |
| Redundancy | Main Redundancy Concepts:<br>- N+x Cold Redundancy (N ≥ 1, x ≥ 1): Use N functionally identical units in the nominal chain; in case of a detectable and isolable fault switch-on x (or 1 of x) and switch-off faulty unit from N.<br>- N+x Hot Redundancy (N ≥ 1, x ≥ 1): Use N functionally identical units in the nominal chain; in case of a detectable and isolable fault ignore e.g. measurement of faulty unit and consider the one of a hot redundant spare unit x. | Fault Management |
| **S** | | |
| Safe Mode | Spacecraft system and/or AOCS mode. Major tasks of safe mode(s) are to provide sufficient power, communication with ground, acceptable thermal conditions, low power and propellant consumption, avoid damage and contamination. See also *Survival Mode.* | AOCS |
| Survival Mode | Alternative term for *Safe Mode*. In case there exist multiple safe modes, they might be differentiated into safe mode(s) and survival mode(s). Survival mode(s) were found to require even less resources compared to the safe mode(s). | AOCS |
| **T** | | |
| **U** | | |

| | | |
|---|---|---|
| Unit | In the context of AOCS a sensor or actuator, e.g. a single star tracker of a single reaction wheel. All units of the same type constitute an equipment (e.g. three start tracker units form the star tracker equipment) and all equipment (pl.) consitudes the equipment set. Alternative expression: device. | AOCS |
| **V** | | |
| Validity Parameter | The term "validity parameter" is used in the PUS-Standard (Service 12) as name for a boolean flag whose value determines whether another variable should be monitored or not. Example: If AOCS is in safe mode then monitor the spacecraft rate against limits of +/-4°/s. The boolean flag telling whether the spacecraft is in safe mode (e.g. isAocsInSafeMode) would in this case be the "validity parameter" for the monitoring function of the spacecraft rate. | FDIR |
| **W**<br>**X**<br>**Y**<br>**Z** | | |

### 7.2.1 Definition of Fault & Failure

Fault & Failure from the Perspective of the AOCS:

- If a fault happens in a unit (i.e. on unit level), it can cause a failure of the unit.
- This failure of the unit is in turn a fault from the perspective of the AOCS (which should not lead to a failure of the whole AOCS).
- A failure of the AOCS would be a fault to the system level.

These relations are illustrated in Figure 7-1.

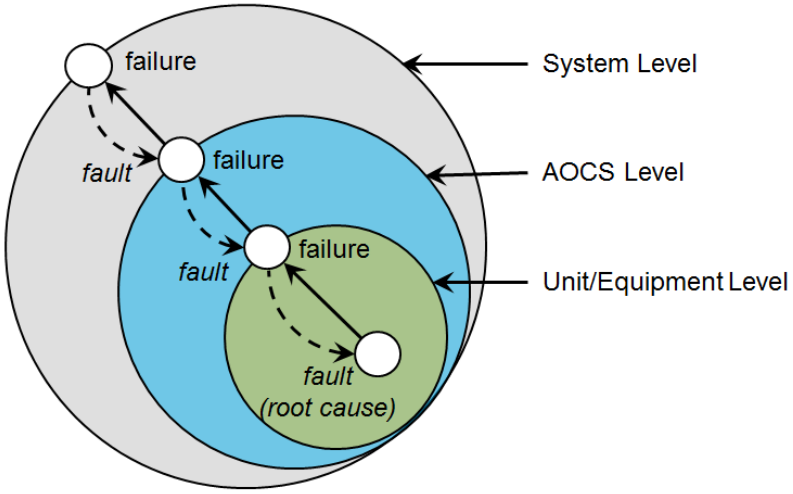


Figure 7-1: Fault & Failure as seen from different levels with different system boundaries. Dashed lines are explanations, solid lines are causations (based on [RD-2]).