GNC 2014: 9th International ESA Conferece on Guidance, Navigation & Control Systems
Porto, Portugal | 2 - 6 June 2014
European Space Agency

FDIR AND ROBUSTNESS FOR THE SOLAR ORBITER AOCS

R. Noteborn[1], L. Stenqvist Hanbury[1], R. Larsson[1], S. Veldman[1], J. Myatt[2], M. Pigg[2], M. Yu[3], A. Prezzavento[3], J. Touaty[3]
[1]OHB Sweden, Sweden. [2]Tessella Ltd., UK, [3]Airbus Defence & Space, UK

ABSTRACT

Solar Orbiter is an ESA Cosmic Vision M-class mission, which is to perform remote sensing and in-situ measurements of the Sun and its environment, from close proximity (down to 0.28AU) and high latitudes out of the ecliptic plane.

A key element in the robustness is protection against high Solar thermal input. Radiators and solar arrays on the spacecraft need to be protected. This limits the angular excursion the spacecraft is allowed to make from Sun pointing. This provides challenges for in particular the detection and recovery of open thruster failures, but also for slow drifts away from the commanded attitude.

The mission features a high degree of autonomy, as the spacecraft is not only autonomously acquiring the Sun in a thruster based mode, but also transitions to wheel based Sun pointing control, after an autonomous wheel health check. Under the right conditions, the star tracker is activated for inertial, wheel based pointing. This results in the spacecraft being able to fully autonomously reach its normal operating mode (gyro-stellar, wheel based control under ground commanded guidance profiles). An alternative path exists in both the thruster based and wheel based control modes to perform a medium gain antenna strobing manoeuvre, ensuring communications with ground.

The Airbus defined FDIR concept is a centralized one, where the AOCS provides monitoring parameters upon which recovery strategies are initiated. Units are monitored on their performance, onboard algorithms are monitored for deviations from normal behaviour and operator inputs are checked for correctness and availability. Important monitoring signals are the Solar aspect angle, as well as the inertial angular rates, being last resort monitors to safe guard the spacecraft from loss of Sun pointing attitude.

The paper concentrates on the FDIR design methods and results. In the design, emphasis is placed on the processing of the unit and subsystem FMECA. This is completed by analysis work to ensure full understanding and coverage of the identified failure modes under different use cases, such as AOCS modes and manoeuvres. This leads to a consolidated set of monitors and recovery actions, and requirements to these monitors and recovery actions are identified. Based on this, the monitors are designed, and prioritized. The prioritization ensures that lower level monitors trigger recovery actions first, as failing equipment can be isolated in that way. When the lower level monitors do not identify failures, then higher level monitors form a second and third line of defence. This prioritization manifests itself in the tuning of thresholds and recovery time outs. The FDIR design is finally verified on several stages of closed loop simulation, ending in HITL campaigns and a final tuning based on final performance predictions for both subsystem and units.

It is also noted that this work has a close interaction with the AOCS control design work, particularly in terms of mode entry conditions for the various modes and boundary constraints for the design, such as rate bounds. The thruster failure detection is based on excessive angular rates, which lead to hard constraints on the control design. However, these constraints can be relaxed when the pointing performance of the various modes improves. This leads to an iterative design, where pointing performance, stability, rate limits, mode entry conditions all contribute to the critical Sun pointing performance under the presence of failures.

1. INTRODUCTION AND BACKGROUND

The ESA Solar Orbiter is an interdisciplinary mission to the Sun. It consists of a single spacecraft which will orbit the Sun in a moderately elliptical orbit, using a suite of advanced Remote-Sensing and In-Situ instruments to perform a detailed observation of the Sun and surrounding space.

The Attitude and Orbit Control Subsystem, or AOCS, constitutes a suite of components that in close interaction with the rest of the spacecraft controls the orientation and stability of the spacecraft, and executes the ground requested velocity changes for adjustment of the otherwise ballistic trajectory. This function includes the monitoring of its own health, as well as the provision of a reference on selected data related to trajectory and orientation, in order to support control of mechanisms.

The European Space Agency (ESA) is the end-customer for the spacecraft. Solar Orbiter is planned as part of ESA Science Directorate's (D/SRE) "Cosmic Vision" programme. ESA will also operate the spacecraft from their facility at ESOC, Darmstadt. Airbus Defence & Space (UK) is the Prime Contractor. The AOCS is subcontracted to OHB Sweden, who is in charge of system engineering, procurement of equipment and software, as well as robustness, simulator and verification engineering. Tessella Ltd (UK) is a subcontractor to OHB Sweden, in charge of the estimation and control design and performance verification. The central elements of the AOCS in the flight software are implemented by Terma AS (DK).

This paper focusses on the Failure Detection, Isolation & Recovery, in so far related to AOCS. First, the mission and the spacecraft are introduced. The onboard autonomous concepts as well as design constraints are discussed, and the FDIR design process is laid out. Special attention is given to the interaction between FDIR and control design. The paper then moves on to show some of the major failure modes and their proposed recovery methods. Some of the more interesting features of the FDIR are discussed in more detail, such as the rate anomaly detection, attitude anomaly detection in non-Sun pointing orientations, and the special attention that the star tracker handling receives in the presence of a solar flare.

2. SOLAR ORBITER MISSION AND SPACECRAFT

The Solar Orbiter mission aims to place a spacecraft in the vicinity of the Sun (as close as 0.28AU) and to high Solar latitudes (minimum 30 deg). To this end, the orbiter is launched with an Atlas booster, with an earliest launch window in January 2017. The mission is entirely ballistic, where a series of Earth and Venus gravity assist manoeuvres will reduce the perihelion distance, as well as increase the orbital inclination. The total duration of the entire mission (up until the end of the Extended Mission Phase) will be approximately ten years. An impression of the orbit of the spacecraft is given in Fig. 1.

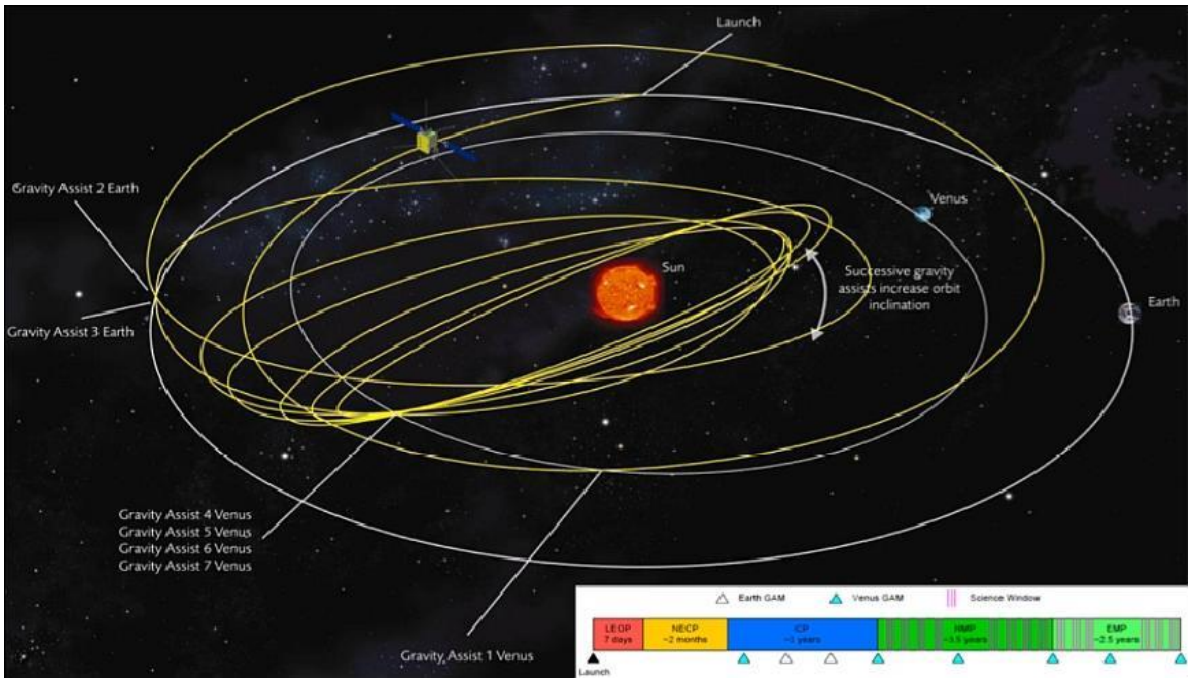

Fig. 1: *Solar Orbiter Trajectory around the Sun. (courtesy ESA).*

The spacecraft design is driven by the large thermal inputs expected at close distance to the Sun. To this end, a heat shield has been designed to keep the spacecraft in shadow, with instruments protruding. The High Gain Antenna can be folded back into the shadow, and the Solar Arrays are canted carefully to limit the amount of direct Solar illumination they receive. This in turn drives the maximum off pointing that can be allowed before the spacecraft is in thermal danger with fatal results for the mission. The off-pointing limitations drive the FDIR design. Another driving aspect of the spacecraft is the radiation tolerance. Especially the star tracker is a unit that is prone to single event upsets. This is to be handled appropriately in the FDIR design, to allow the spacecraft to operate (without using redundancy) in this natural environment.

A set of primary requirements to the AOCS are:

- Maximum 6.5 deg off-pointing from the Sun, with maximum 50s off-pointing over 2.3 deg
- Capacity of fine pointing without star tracker measurements for at least 24 hours
- A fine pointing Absolute Pointing Error of 42 arcsec, with an Attitude Knowledge Error of 25 arcsec. The Pointing Drift Error is specified at 13 arcsec over 24 hours, using 10s integration windows. All figures are applicable to Line of Sight to the Sun, 95% confidence.

Key features of the spacecraft are a mass of around 1800kg and a span of about 17.5m. An artist's impression of the spacecraft in flight is shown in Fig. 2.

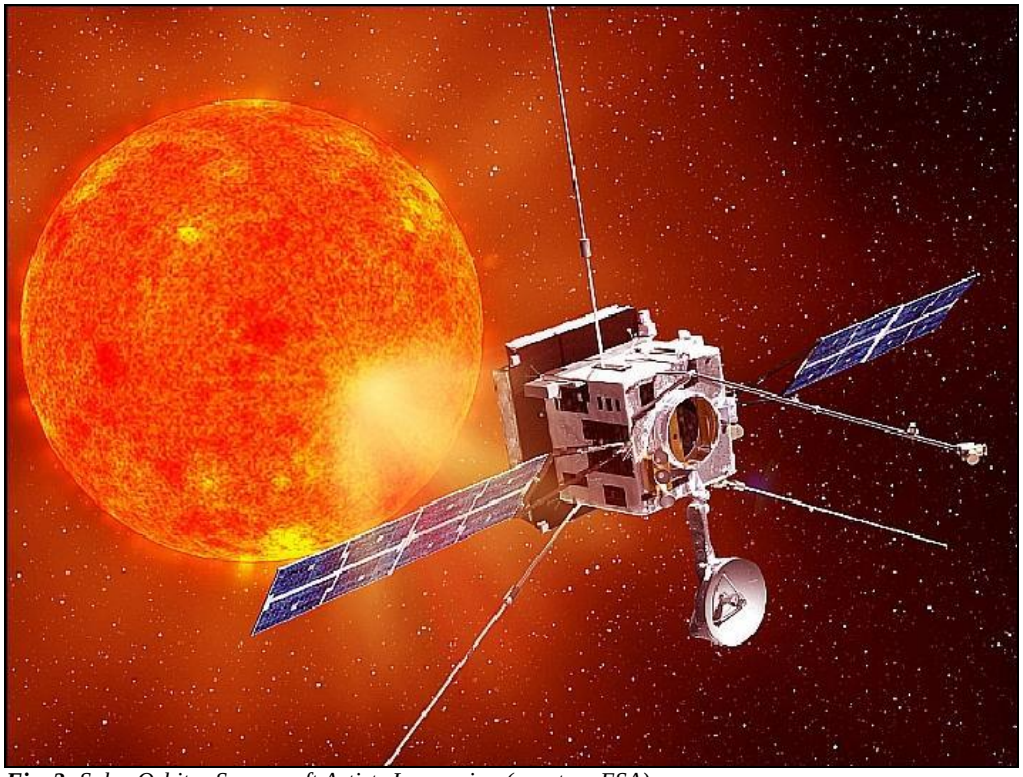

Fig. 2: *Solar Orbiter Spacecraft Artists Impression (courtesy ESA).*

The AOCS consists of most of the classical elements found on interplanetary missions, but with the special feature that the onboard computer handles all tasks, such as data handling, thermal control, AOCS and FDIR, on a single processing module. The equipment used are two pairs of Fine Sun Sensors, two Inertial Measurement Units, two Star Trackers, four Reaction Wheels, and a redundant bi-propellant propulsion system consisting of 9 thrusters per branch. The Inertial Measurement Units consist of one nominal branch featuring high performance rate measurements from four tetrahedron oriented gyroscopes and a contingency branch providing reduced rate measurement performance. The nominal branch also includes four tetrahedron oriented accelerometer channels. All units are communicated with via two MIL-1553B redundant busses. The units are synchronized to the onboard time reference at a minimum of 8Hz data acquisition, corresponding to the attitude control frequency.

The AOCS is organized in five modes, each comprising of several submodes to accomplish specific tasks. These modes are defined by Prime, as listed in Table 1 and illustrated in Fig. 3. The SASM and WSM also provide a contingency operation called Earth strobing, which consists of a configurable rotating motion about the Sun line, to be stopped by ground when the Medium Gain Antenna (MGA) points to Earth.

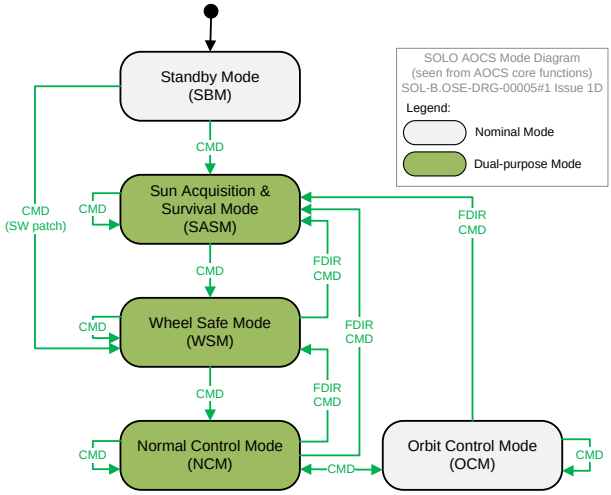

Fig. 3: *AOCS Mode Diagram.*

Table 1: *AOCS Mode Definition.*

Mode	**Function**	**Means**
Standby Mode (SBM)	Basic unit data processing, is entered after reboot.	No state estimation, no actuation.
Sun Acquisition and Survival Mode (SASM)	Providing the capacity of rate damping, holding in eclipse, Sun search scanning rotations, autonomous Sun Capture and Pointing.	Sun referenced and gyro referenced, thruster actuated.
Wheel Safe Mode (WSM)	As for SASM, but lacking the capacity of rate damping, Sun search and Sun capture for smaller angles only. To be entered from SASM, or NCM.	Same as for SASM, but wheel actuated.
Normal Control Mode (NCM)	Full three axis control, used as the principal operating mode during cruise as well as for scientific observations.	Gyro-stellar estimation, wheel based control, inertially referenced.
Orbit Control Mode (OCM)	Full three axis control, with the added functionality of providing a delta V for orbit control. This mode is also used for Earth flyby, taking advantage of the increased torque capacity compared to NCM.	Same as for NCM, but thruster actuated.

3. ONBOARD AUTONOMY & DESIGN CONSTRAINTS

The Onboard Autonomy concept, and the associated FDIR principles are specified by Prime. They can be summarized as follows. The FDIR is a centralized system. The subsystems report their own and their components' health by means of monitoring signals. These monitors are connected to the triggering of individual recovery actions. Such actions can be the switch of units to their cold redundant branches, or applying three out of four hot redundancy. On subsystem level, recoveries can include switching of estimation methods or fall back in modes. The FDIR also has the option to include a processor reboot as part of the mode fall back and branch switching, depending on the monitor triggering the recovery.

The recoveries are divided into five levels, and these are now discussed from an AOCS perspective. The lowest level (Level 1) is the FDIR that is internal to the equipment, which usually includes such measures as under-voltage and overcurrent protection. This is monitored by the AOCS, such that redundant units can be configured in case of a unit entering a fail safe mode. Level 2 includes performance monitoring of the units by the AOCS, but also monitoring of the control and estimation algorithms. The recovery includes the reconfiguration to redundant units, but also mode fall back or reconfiguration of the algorithms. In these cases, the monitors are always very straightforward connected to the cause of the failure. However, on level 3, the monitors are more generic and direct in nature. They may monitor the Sun angle or the angular rate, and since in this case the failure cause is not straight forward, a mode fall back to Sun Acquisition is accompanied by a reboot of the

Processor Module. Depending on the trigger, redundant branches of equipment are configured. A schematic overview of the process is displayed in Fig. 4. In the diagram, only the first three levels are pictured, as they are relevant to the AOCS. The fourth one is greyed out as the AOCS does not participate in this level. A fifth level exists, which is the interaction with ground. This level is not displayed as it is not part of the onboard autonomy.

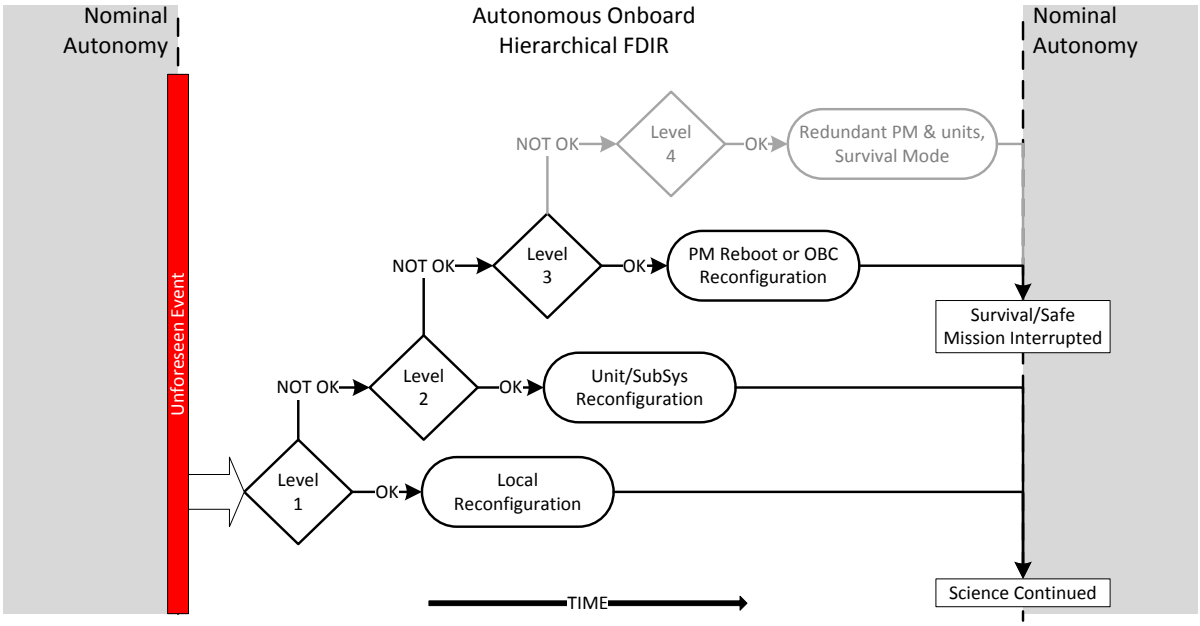

***Fig. 4**: FDIR Levels (free after Airbus DS concept).*

Besides the autonomous fall back to lower modes and the use of redundant equipment, the Solar Orbiter FDIR also features the capacity to bring the spacecraft to the highest possible state of operations, available with the selected hardware. When the AOCS has completed the Sun acquisition, the FDIR requests an autonomous check out of the healthy Reaction Wheels. At completion of this check out, the FDIR decides on the presence of at least three healthy wheels, enabling it to switch thruster based SASM operations, for wheel based WSM control. This provides for the reduction of propellant usage. In case an insufficient number of wheels is available, the mode is not switched, but instead the spacecraft is brought into a rolling motion about the Sun line. The Medium Gain Antenna (MGA) is angled at the expected Sun-Earth angle (maintained by ground). The rolling motion will periodically "strobe" the MGA lobe to the Earth, and ground can stop this rotation at a convenient time, thereby establishing contact via the MGA.

In WSM, the FDIR has the possibility to request from AOCS an autonomous Star Tracker check-out. The Gyro-Stellar Estimator is initialized in this checkout, thereby providing an inertial state estimate. If the FDIR decides that the check-out was successful, it can change the AOCS mode to NCM, thereby establishing a fully three axis inertially stabilized platform. This provides for optimal operations, especially the possibility to point the High Gain Antenna (HGA) to the Earth using ground-configured ephemeris functions and attitude guidance reference profiles. In case the Star Tracker check-out does not succeed, the FDIR will again initiate the same strobing manoeuvre as for SASM. This eventually provides for communications via the MGA.

It follows that the FDIR onboard Solar Orbiter is both capable of handling anomaly situations in returning the spacecraft to a safe state, but also of reducing the amount of contingency operations traditionally taken care of by ground, by proceeding with mode advances as long as the required hardware clears the spacecraft built-in tests.

4. DESIGN PROCESS AND INTERACTION BETWEEN FDIR AND CONTROL DESIGN

OHB Sweden developed a process to design the FDIR components required for the Solar Orbiter safety and success of the mission. This process aims at formulating the monitors (both those part of the AOCS as well as those outside, supporting the AOCS) and associated recovery actions. These design elements are then implemented in software to become part of the flight functionality. A conceptual overview of the elements in this process is given in Fig. 5.

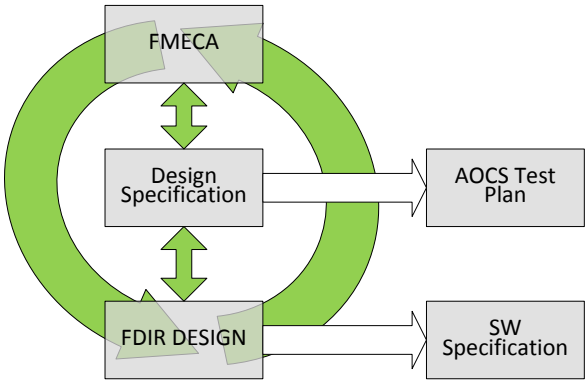

***Fig. 5**: Conceptual overview of the OHB FDIR design process regarding its interaction with other processes.*

The FDIR design activities are performed in an iterative way, and focus on resolving identified failure modes. As such, the Failure Mode, Effects and Cause Analysis (FMECA) is a central element in the FDIR design. The unit suppliers provide FMECA reports on their units, with suggested monitorings and recovery actions. Prime identifies selected failure modes for elements under their control and specifies these to the AOCS contractor. Failure modes that arise in the subsystem itself are defined by the AOCS contractor, including software specific failure modes identified by the SW supplier. The FMECA is then consolidated and unified by producing the subsystem FMECA, which is a list of all relevant failure modes in units, spacecraft elements related to AOCS, and the identified failure modes on subsystem/software level. At this point in time, it is possible to extract a list of monitors, preventative measures and recovery actions, available as the first issue of the FMECA document. Completeness of these measures is obtained by observing that each failure mode is covered.

It deserves to be mentioned here that in order to identify the failure modes of the subsystem itself, a Functional Analysis is used as input. This analysis breaks down all functions of the AOCS, and links them together using identified inputs and outputs. Following the stream of information in these functional blocks allows for the listing of failure modes, to be expected in the control system itself.

A design based on individual failure modes is not considered optimal. Neither is it possible to show that all the possible situations that the spacecraft encounters, are covered appropriately. The FDIR design is now started by means of an analysis. This analysis covers the following aspects:

- Unit Internal FDIR and recoveries are reviewed and reported upon in the FDIR report. A unit may take specific actions in case of failures, and these need to be compatible with the FDIR philosophy. If a unit reboots, or switches itself off, then the AOCS needs to be robust to that. It is important to understand what the units do autonomously in which situation, how that can be observed and which actions the AOCS needs to take in order to cope with the situation and continue its controlling functionality. This analysis may lead to modification or formulation of new monitors and recovery actions.
- The applicability of failure modes under different phases in the mission, different modes or different spacecraft dynamics, is reviewed. Certain failure modes may only be observable under specific circumstances. A monitor may have constraints that prevent it from being used in all situations. A recovery action proposed in the FMECA, may have consequences or may not be appropriate under given circumstances. This analysis modifies the list of monitors and recoveries, consolidating the design further.
- Duplications or unnecessary complexity of the monitor and recovery action list is a natural result of the failure by failure case analysis of the FMECA. Reviewing the monitor list as a whole reveals duplications and overlaps. This analysis streamlines the list of monitors and recovery actions, economizing the design.

When this analysis is complete, the list of monitors, preventative measures and recovery actions has been updated. This allows for a new issue of the FMECA, which is brought in line with the FDIR design. This analysis may also have brought to light certain requirements to the monitors or recovery actions. The FDIR

design report lists these requirements, as input to the specific monitor design. Also operational constraints may be identified here.

As a final step, the individual monitors are designed, and this is documented in the report.

During this design process, constraints may be identified to the control system. The control system is for instance to be robust to temporary data outages (during unit reconfiguration), and to a change in the units (different alignment or change in bias for example). These constraints are identified in the FDIR design report. Another type of constraints is the mode entry conditions. The worst case dynamic conditions for each mode entry are determined following an analysis that identifies all reasons for a mode entry. Apart from the nominal ground commanded mode transitions, the onboard FDIR commands a change of mode following conditions that are the outcome of the FDIR design. It turns out that this is one of the most complex interactions between control design and FDIR design, as the two depend on each other. This means that the mode entry conditions are part of an iterative work flow.

In order to introduce the FDIR design to the different disciplines in the project, the Subsystem Design Specification (SDS) is updated with requirements that reflect the needs of the FDIR. This allows for the following:

- The requirements call for instance for the identified monitors to be implemented. As the software requirements specification, being the baseline for the SW supplier activities, is traced to the SDS, it becomes possible to ensure that each element of the FDIR is properly implemented in software. The FDIR design report also includes trace tables that show how specific aspects of the design are represented in the SW requirements, as the design report includes more details than the SDS.
- The FMECA monitors, preventative measures and recovery actions are traced, where applicable, to SDS requirements. As these elements are coupled to failure modes, this makes it possible to demonstrate that each failure mode is covered. Elements that are not implemented under responsibility of the AOCS contractor, but instead by Prime, are traced to the PA Critical Item List.
- Each SDS requirement is to be verified, and the trace to for instance the AOCS Test Plan will identify where verification of each FDIR element takes place during Qualification and Acceptance testing of the AOCS.
- The FDIR constraints to the control system are included as SDS requirements. As the SDS applies to all elements of the AOCS (excluding the hardware), these requirements are automatically driving the control system design towards a compatible solution with the FDIR. Also here, the verification follows the requirements.

In order to make this process smooth and time-efficient, the use of Doors requirements management software has been found invaluable. Not only the requirements are captured in Doors, but also the full FMECA and the Test Plan are stored as Doors modules, allowing all elements to be linked. This gives the possibility to consistently present the information from multiple view points.

5. ROBUSTNESS OF CONTROL SYSTEM

In the preceding section, an outcome of the FDIR design was the formulation of constraints towards the control system design. As units experience failures, checks identify data as invalid, and units are generally unavailable due to failures or reconfigurations in progress, the control system must remain robust and proceed to function in controlling the spacecraft. Generally, one could say that the control system must be robust against absence of input data from sensors and actuators, or even operators, or the unavailability of control authority.

As a result of these considerations, the control system is built up in terms of layers, which is illustrated in Fig. 6. The raw sensor and actuator data that comes in on the lowest layer is validated by means of checks directly on the unit data. The results of these checks are reported as monitoring signals, so FDIR can respond with recovery actions. However, until that recovery action takes place, the control system operates on either replaced data, or the data is clearly marked as invalid. This allows the middle layer, where state estimation takes place, to take the appropriate action. Estimators may be able to propagate, or the estimated states can be marked as invalid if no alternative estimation technique is available. In practice, the latter only happens if no valid gyroscope data is available. Also in this layer, checks are being performed and reported as monitors. This enables the FDIR to respond for instance to inconsistencies between data of different sensors, or excessively long periods of state propagation. The final layer implements the control and outputs control demands. Monitors are used here to for instance check on the achievement of control objectives. Control is typically suspended if no valid state

estimation is available. The requirement placed on the control system is to be able to cope with interruptions of valid state estimates, and therefore of suspended control, of up to 10s (order of magnitude of the hardware reconfiguration time).

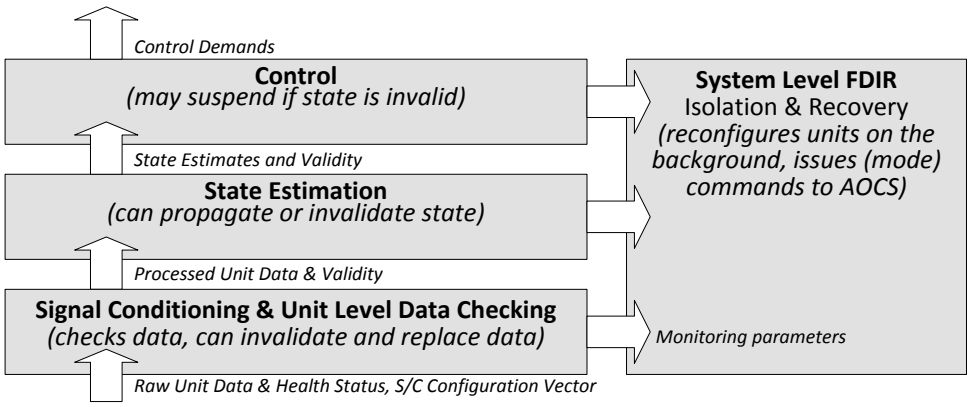

Fig. 6: *Layered concept of the Control System with hierarchical data validation and replacement.*

6. RATE ANOMALY DUE TO OPEN THRUSTER FAILURE

One of the major anomalies onboard is an open thruster failure. All but one of the thrusters on each branch contribute to torque, causing worst case angular accelerations in the order of 0.6 deg/s^2. This kind of anomaly develops quickly into an angular rate on the spacecraft and therefore also a Sun angle builds up. This Sun angle is critical in the thermal protection of the spacecraft.

On Solar Orbiter, a direct way of monitoring thruster failures is to monitor the angular rates. However, in order to prevent Sun angle building up, the rate threshold is to be limited. During Sun acquisitions from arbitrary orientations the angular rates can be very high, and a suitable rate threshold cannot be found. The remaining time of the mission, the angular rates are very low and thus can be monitored in order to trigger a thruster failure recovery: the Rate Anomaly Detector, or RAD. In order to demonstrate compliance to the 6.5 deg maximum off pointing requirement, a time line was created. This ranges from a worst case initial state through failure detection, and an angular drift of the spacecraft while thrusters are being reconfigured. Finally, the SASM control is re-activated, which reverses the rate and re-acquires the Sun.

Table 2 illustrates the time line of an open thruster failure using a RAD threshold of 0.3 deg/s. Several parameters were found to be critical in this sequence. The rate violation has a drastic recovery action, and is therefore to occur twice to avoid false alarms (spikes). Being able to sample angular rates faster than the control frequency reduces the reaction time between first and second detection of the rate violation. Therefore the gyroscopes are sampled at 16Hz, rather than at the 8Hz control frequency. Another important factor is the thruster reconfiguration time, in which no control is possible. In fact, wheels are running down on friction causing a low but significant amount of acceleration on the spacecraft. It proved to be important to be able to start the SASM as soon as possible, which is done by direct mode transition, rather than to wait for a full reboot of the Processor Module. A full recovery of the Processor Module increases the coasting time, which would again limit the rate threshold severely. The bottom limit of the rate threshold is formed by the feasible performances of the thruster based control, under the constraints of given spacecraft plant and actuator performance.

Table 2*: Open Thruster Failure Time Line illustrating angle drift until rate reversal (times at end of event).*

Event	Comment	Time [s]	Rate [°/s]	Angle [°]
1st RAD Detection	RAD required to trigger twice at 16Hz	0.7461	0.3843	0.1526
2nd RAD Detection	Recovery is started here	0.8086	0.4185	0.1792
SASM entry	Rate reduction starts	7.1086	0.5416	3.5272
Rate reversed	Sun acquisition starts	8.1561	0.0266	3.8450

The selection of the rate threshold in itself turns out to be a complicated process. Any selection of the threshold leads to a defined angle drift value. Combined with an initial angle, the time line gives a remaining margin to the 6.5 deg limit. Shorter recovery times and better initial angle (read better pointing performance) allow for larger rate thresholds. The maximum allowed RAD threshold becomes then a function of the initial worst case

angle (itself a function of the APE). The critical case was found to be the thruster-based OCM, where spacecraft rates are the most extreme and pointing performance is lower compared to wheel-based modes. In this case, the required pointing performance is driven from another FDIR monitor (Attitude Anomaly Detector), and this leads to the selection of the RAD limit. Both pointing and rate worst case performances are thereby driven by FDIR constraints.

7. ATTITUDE ANOMALY IN NON-SUN POINTING ORIENTATIONS

As the nature of the mission drives the spacecraft to be Sun-pointing all of the time, using a Sun sensor as an independent monitor of the Sun angle becomes an obvious design for the modes that are Gyro-stellar based. This concept is called the Attitude Anomaly Detector, or AAD. However, the FDIR design iterations reveal that there are operational phases that are unprotected. These include eclipse and non-Sun pointing operations. The latter are performed for optimal delta-V manoeuvres on distances further than 0.95AU where thermal constraints are relaxed. In these operations, the Sun sensors do not see the Sun and are therefore not available as an alarm, whereas the possible relevant failure modes cannot be ruled out. An alternative solution is to use the Sun angle from the Gyro-FSS Estimator, which blends gyroscope rates with Sun sensor angles and is able to propagate in the absence of Sun sensor data.

In this case, an analysis was performed to ensure full protection from the failure modes by reviewing them. The AAD protects against slow drifts away from the Sun, but this is not relevant in the non-Sun pointing operations. Here, operator error in guidance profiles would be unprotected, as the spacecraft would follow any well-formed reference. To protect from this error, the spacecraft performs a Sun angle check. The Sun angle is computed based on an onboard (and independent) profile for inertial Sun direction, and the inertial spacecraft reference orientation from the guidance profile to be checked. This computed Sun angle must match a ground configured "expected Sun angle". This is in principal a single axis solution, which could be extended to three dimensional by computing an "expected Earth angle" as well.

Gyroscope rate measurement performance can be reduced as a consequence from specific failure modes. This is observable from a comparison between gyroscope channels, but a certain measurement error cannot be avoided in that way. However, this error is bounded, and given the durations of the operations/eclipses, an off pointing prediction can be made and assessed.

The gyroscope has failure modes that reduce its measurement accuracy. This reduction can be observed/detected by comparing between gyroscope channels but a residual error would be tolerated by this check. As this residual is known as well as the durations of the operations/eclipses, the resulting off- pointing can be assessed and deemed tolerable.

A final measure to complete the protection of the spacecraft without AAD is the monitoring of the angular control error. This control error is expected to be bounded in NCM and OCM, as any initial entry control error is eliminated by a compensating slew computed by onboard guidance. A control error can then only exceed thresholds if either the guidance or state estimation indicates a sudden excursion. Guidance can be ruled out, but state estimation could show an offset angle due to real motion, sensor failure or filter problems. All of these would be detected by an AAD, but can also be detected by comparing to guidance reference via the control error.

In conclusion it proved that operations without the AAD can be made fully protected. When it is available, however, the AAD is the most direct measure of off-pointing (indicator of an off-pointing) and is therefore maintained.

8. STAR TRACKER SOLAR FLARE HANDLING

As already introduced, the Solar Orbiter spacecraft travels in zones of high radiation. Sudden eruptions of energy from the Sun can lead to a hostile environment for, among others, the Star Tracker, leaving it blinded for a day or longer. As the spacecraft is experiencing these environments especially during the periods where it is performing its scientific observations, the effect of solar flares cannot be considered a failure. The consequence of that principle is that when a Star Tracker is out of operation due to solar flare impact, it cannot simply be switched to its redundant unit, as the redundancy then has been consumed. Should that redundant Star Tracker fail for whatever reason, there is no other Star Tracker to turn to. In addition, if the redundant unit would be selected, it is likely that it has the same solar flare induced problem, and so FDIR would soon have no options

left. The solar flare is a temporary phenomenon, and so the Star Tracker is expected to return back to operation after the Solar Flare has reduced in intensity.

The monitors and recoveries for the Star Tracker have in first iteration been arrived at on the basis of the list of failure modes, and been evaluated in the light of the STR internal FDIR. Table 3 gives a list of these monitors and recoveries. As the Star Tracker is an intelligent unit, it can display quite a few autonomous responses, making design of the monitors and recoveries more complicated compared to the other units. For instance, when the Star Tracker spontaneously reboots, then the data flow stops for many control cycles. Normally, lack of response from a unit is directly recovered from by switching to redundancy, but in the case of an SEU in the Star Tracker, this reboot should be allowed. The recovery action in this case is to stop the spontaneous reboot by a power cycle, and perform a controlled reboot. This is required, as the unit needs to be configured by a sequence of commands, which will not occur if the reboot is performed by the unit in the background and the AOCS ignores it.

Table 3: *Star Tracker Monitors, their sensitivity to solar flares, and recovery actions.*

Monitor	**Solar Flare Sensitive**	**Recommended Recovery Action**
Bus Communication Check	YES	In case of lack of communication, but no sign of 1553 failure: STR reset with direct NEAT entry
STR Timetag Freezing Check	NO	Switch to redundant STR.
STR Mode Check	NO	INI: switch to redundant STR
	YES	STB: command to AAD and perform retries.
	N/A	AAD: No action
	N/A	NEAT: No action
	NO	Other: switch to redundant STR.
STR Time Sync Check	NO	Switch to redundant sync interface and send the time update TC. If not available, switch off STR and activate the redundant STR.
STR Attitude Validity Check	YES	Direct NEAT entry
STR HK Check	NO	Switch to redundant STR. This is not solar flare prone and can therefore use redundancy.
STR-GYR Consistency	YES	STR reset with direct NEAT entry

The Star Tracker can be commanded directly to its tracking mode if it is supplied with a sufficiently accurate seed of the attitude estimate. Except for WSM, where the transition is made from Sun referenced control to inertial control, the seed is available from the Gyro-Stellar Estimate. In case of solar flares, the seed gives the Star Tracker a very high chance of success in returning to its tracking mode. Therefore, the Star Tracker recovery actions are based on the seeding function. The monitors that detect the effects of solar flares all lead to such an aided start-up.

The overall design of the Star Tracker handling is complicated by the fact that even though a monitor is solar flare sensitive, its triggering for recovery does not necessarily mean the cause of the monitor triggering was a solar flare. So eventually, redundancy is expected to be used. Therefore, the consortium designed a hierarchical recovery approach. This approach is described here, from the bottom level upwards:

- The AOCS monitors are allowed to trigger until their recovery time-out has passed. At that point, the associated recovery is initiated.
- For non-solar flare sensitive monitors, the FDIR declares a unit unhealthy, which leads to activation of the redundant unit.
- For solar flare sensitive monitors, the FDIR decreases the health status of the Star Tracker that is being used for control. The recovery is then begun by selecting and activating the unit that has the highest health status. This usually means a power cycle, activation sequence, followed by a seeding command to start tracking.
- This cycling does not result in an unhealthy declaration of any Star Tracker, as there is a minimum health status that cannot be reduced further.
- As the AOCS is designed to tolerate absence of the Star Tracker measurements for up to 24 hours (in NCM), the autonomous recoveries and switching of the Star Tracker continue until this rate propagation period times out. At that point, the FDIR commands a mode fall back to WSM. In OCM,

there will have been sufficient time to complete the delta V. From OCM, being a thruster based mode, a thruster based Sun acquisition in SASM is performed after STR propagation time out.

- The highest level of recovery consists of the Star Tracker check out already described in section 3. In case the Star Tracker is found to be functioning correct, the Gyro-Stellar Estimator will have converged and the system is ready to go back to inertial control. If the Star Tracker is deemed unfit, the strobing is started.

9. CONCLUSION

The Solar Orbiter AOCS is now ending its design phase, running up to design reviews, with the first flight software increments (signal conditioning and initial FDIR elements) being delivered. The next phase will see the qualification testing and flight tuning of the AOCS FDIR, followed by its acceptance testing.

This paper has described the Solar Orbiter AOCS FDIR design in terms of its driving requirements, design process, interaction with the control design and performance. The autonomy concept of the spacecraft was presented, and how the FDIR design fits in with that. Special examples were highlighted. The design is believed to give a solid basis for the autonomous operations and the safety of the mission, which will be confirmed when the project moves over to its verification stage.

ACKNOWLEDGMENTS

The authors would like to thank the following people that have contributed to the design of the Solar Orbiter AOCS FDIR: Ilario Cantiello from Airbus DS, and Jacques Rouquet and Benedicte Girouart from ESA/ESTEC. This acknowledgement does not imply the endorsement of ESA to the views presented in this paper or the associated conference presentation.