Sādhanā, Vol. 11, Parts 1 & 2, October 1987, pp. 233–261. © Printed in India.

Fault-tolerant spacecraft attitude control system

S MURUGESAN and P S GOEL

Control Systems Division, ISRO Satellite Centre, Bangalore 560 017, India

Abstract. Spacecraft perform a variety of useful tasks in our day-to-day life. These are such that spacecraft need to function properly without interruptions for 7 to 15 years in space without any maintenance. Though most spacecraft have redundant systems to serve as back-ups in case of failures, they greatly depend on human assistance through ground stations for failure analysis, remedial actions and redundancy management, resulting in interruption in services rendered. There is, therefore, need for a fault-tolerant system that functions despite failures and takes remedial action, without human assistance/intervention, autonomously on board the spacecraft.

Commonly used techniques for fault-tolerance in computers cannot be directly used for fault-tolerance in sensors and actuators of a closed loop control system. Further, for space applications fault-tolerance needs to be achieved without much penalty in weight and computational requirements.

This paper describes briefly the attitude control system (ACS) of a spacecraft and highlights the essential features of a fault-tolerant control system. Schemes for fault tolerance in sensors and actuators are presented with an analysis on various failure modes and their effects. Newly developed fault-detection, identification and reconfiguration (FDIR) algorithms for various elements of ACS are described in detail. Also an optimum symmetrically skewed configuration for the attitude reference system using dynamically tuned gyros is developed.

Some of the schemes have already been used in Indian Spaceçraft. As future Indian space missions will directly cater to various applications on an operational basis, the ultimate objective is to have a totally fault-tolerant 'intelligent' autonomous spacecraft.

Keywords. Spacecraft; fault-tolerant control; autonomous reconfiguration; fault tolerance; attitude control; gyros; attitude reference system.

1. Introduction

"It is a feature of most, if not all, control systems that they are only really noticed when they go wrong"

— *A J Sarnecki*

"Be prepared for the unexpected"

— *Motto of US Scout*

"Better put a strong fence round the top of the cliff than an ambulance down the valley"

— *Unknown*

Attitude control of spacecraft is the process of orienting and maintaining the spacecraft and/or the application payloads – such as cameras, antennae, and radiometers – in a desired direction. The satellite's axes inclination with respect to a reference is called the satellite's attitude or orientation. Attitude control is also required to orient solar panels for maximum power generation, to maintain the desired thermal conditions within the spacecraft and to cater to any other specific requirements like having the very high resolution radiometer (VHRR) cooler looking away from the sun.

The attitude control system (ACS), the heart of a spacecraft, consists of various types of sensors and actuators, and control electronics (on-board computer). The control electronics process attitude information from sensors according to given control strategies and generate control signals for actuators to correct attitude errors, if any. Modern spacecraft that render a variety of sophisticated services impose stringent requirements on attitude accuracy and jitter (attitude rate) and consequently the ACS becomes very complex. Also, the long life of space missions (10 to 15 years) significantly influence the system design and operation.

In our modern society, spacecraft play many important roles, domestic and international telecommunication and broadcasting, weather forecasting (meteorology), remote sensing, reconnaissance (military applications) etc. and their services have become essential in our day-to-day life. Hence, there is a growing need to provide uninterrupted operation of spacecraft over very long periods of 10 to 15 years. Therefore, ACS need to be highly reliable and provide uninterrupted operation, in addition to meeting other stringent performance requirements.

However, despite various efforts to improve reliability of a system through 'fault-avoidance' techniques such as improvements in design and fabrication, use of high reliability and burnt-in or screened components and elaborate and intensive testing, failures do occur in various subsystems during their long operational life. Failure of even one of the components/subsystems might lead to malfunction of the entire control system which, in turn, might result in aborting the mission. Effects of failures may range from an interruption in service for a few days and degraded performance to catastrophic ending of the mission.

1.1 *Need for an autonomous fault-tolerant system*

Most of the earlier and current spacecraft control systems generally have redundant units/subsystems to achieve required reliability and to mitigate mission critical 'single-point-failures'. They are, however, greatly dependent on ground support for decision making and management of redundant units. Diagnosis and adaption to faults is carried out by mission/subsystem specialists on ground through careful analysis of various performance and status information telemetered (transmitted) to the ground. Depending on the nature of fault(s) remedial actions are taken through telecommands to effect recovery and to bring the spacecraft back to normal operations. But this approach is not suitable for complex spacecraft and invariably leads to attitude loss and interruption in service which is not tolerable in many applications. Also, there are attendant risks of attitude reacquisition and fuel penalty. Further, this approach suffers from the following limitations:

(1) Due to inherent delays in taking corrective actions from ground, failures such as free flow of fuel through thrusters and the speed of reaction/momentum wheel going beyond its absolute maximum limits, might lead to catastrophic effects.
(2) As in low earth remote sensing satellites, spacecraft may not be 'visible' from ground station(s) all the time to take corrective measures. For deep space missions, interactive control is not possible because of the very long time (about 30 minutes) taken for information travel.
(3) Also, before corrective action is taken the attitude might have been lost necessitating 'reacquisition' of the attitude. Reacquisition attitude is not an easy exercise, especially in the absence of a global network of ground stations, and might take a few hours to a couple of days interrupting the utility of the mission.
(4) In a crisis like a natural calamity, or an external threat, when continued spacecraft operational support would be required more than ever, ground contact and control could be interrupted for long periods.

Thus, there is need to design and incorporate a fault-tolerant control system that performs its functions autonomously despite failures. This can be achieved using redundant subsystems and detecting behaviour of subsystems on board the spacecraft, with full autonomy to switch automatically to redundant units in case of failures. This approach also simplifies ground station operations significantly.

1.2 *Fault-tolerance in the control system*

The fault-tolerance approach accepts the inevitability of failures and counteracts the effect of failures through functional redundancy. It is a "fault-management" technique. Functional redundancy may be achieved either by repeated execution (temporal) or replicated hardware and software (physical). Fault-tolerant systems automatically maintain correct operation of the system despite failures without human intervention. They also have better reliability and system integrity than is achievable by fault avoidance.

The concept of fault-tolerance is not new and a lot of techniques have been developed for fault-tolerance in computer hardware and software (Avizienis 1976; Rennels 1978; Bennets 1979; Siewiorek & Swaz 1981). Since failure modes and redundancy management of sensors and actuators are quite different from that of the computer/control electronics systems, widely used fault-tolerant computing techniques are not directly applicable to sensors and actuators. For instance, actuators that failed in a continuous actuating mode cannot be left as such by substituting a redundant actuator, as is usually done in computers/control electronics. The popular triple modular redundancy (TMR) with majority-voting is also not applicable to actuators like reaction/momentum wheels.

Also, space applications impose severe constraints on weight, volume, power consumption and location for mounting sensors/actuators. Hence, the number of redundant units – degree of redundancy – have to be kept to a minimum. On-board fault detection and identification algorithms for actuators and sensors should be simple for implementation without much increase in hardware, software and run-time overheads. In addition, it is desirable that these algorithms are based on existing performance measurements, without need for additional monitors/transducers.

The basic principle of an autonomous fault-tolerant control system is to prevent a faulty unit from having any further effect and to automatically substitute a redundant subsystem in place of the failed unit before failure results in unacceptable performance. Thus, this strategy enables the system to continue to perform its function without interruption even in case of failures. An autonomous fault-tolerant attitude control system besides performing the normal attitude control functions does the following on board the spacecraft: i) monitors performance of its various subsystems, ii) detects and identifies failures, if any, and iii) reconfigures the subsystem (substitutes a redundant module) automatically on board the spacecraft.

A fault-tolerant attitude control system by tolerating failures in sensors, actuatôrs and control electronics, ensures correct operation inspite of failures; it gives uninterrupted performance and enhances the reliability, the life of the spacecraft and the probability of mission success.

But, as yet, not many spacecraft have autonomous fault-tolerance features. This perhaps may be due to the complexity of fault-detection and identification algorithms proposed earlier and the feasibility of only limited on-board computations. Now, however, with the availability of high performance microprocessors and reasonably simple algorithms it is possible to have an autonomous fault-tolerant spacecraft attitude control system. In the following, with a brief discussion on various subsystems of ACS, we highlight essential requirements of a fault-tolerant control system and discuss some simple schemes for fault-tolerance in attitude sensors and actuators. Fault-tolerant computers/electronics have been discussed quite extensively elsewhere (Avizienis 1976; Rennels 1978; Bennets 1979; Siewiorek & Swaz 1981).

2. Basics of spacecraft attitude control

The attitude control systems orients and maintains the spacecraft at the desired state in spite of disturbance torques and other perturbations on the spacecraft. The life of the attitude control components/elements essentially decides the operational life of a spacecraft. Attitude control of a spacecraft is a classical closed-loop control problem and figure 1 gives the functional relationship between the various elements of ACS and their inputs/outputs. The input reference gives the desired state of the system; the actual state of the system measured by attitude sensors forms the feedback signal. The difference between the reference and the feedback signal is the error signal indicating deviation between the desired and the actual state.

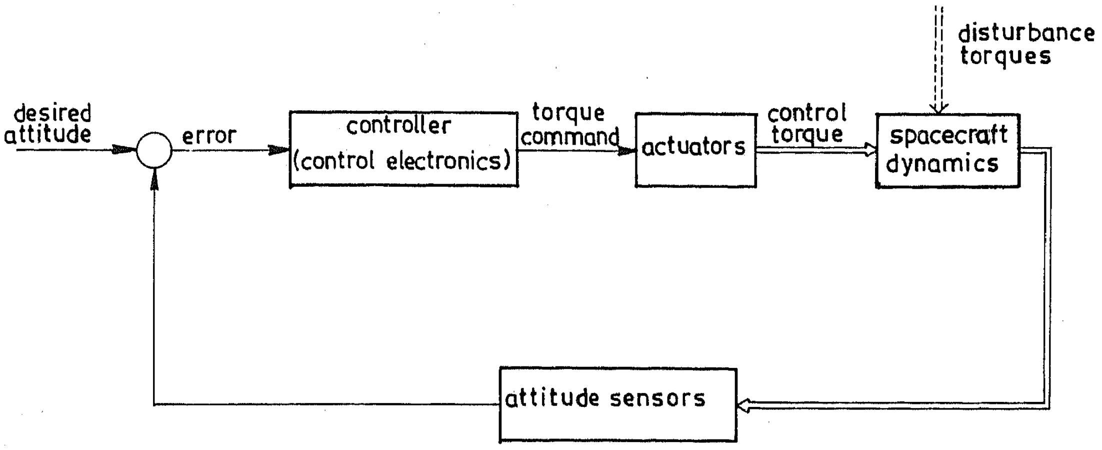


Figure 1. Block schematic of spacecraft attitude control systems.

Generally, attitude measurement is related directly to desired orientation, and hence attitude sensors' outputs directly give the error signal.

The controller generates actuating signals to torquing devices/actuators, based on the error signal and according to 'control laws' that give the desired overall system-performance. Actuators generate torque/force in the desired direction under command from the controller. The spacecraft dynamics gives the relationship between the motion of the spacecraft and the torque/forces (either intentionally generated or disturbance) affecting the motion; it forms a part of the control system. The dynamic behaviour of the spacecraft is generally determined by its physical characteristics like moment of inertia, static/dynamic unbalance etc.

One would expect little disturbance to a spacecraft once the spacecraft is in orbit. However, there are several sources of disturbance torques/forces: aerodynamic pressure, solar radiation, magnetic effects, gravity gradience and internal disturbances, which tend to turn the spacecraft away from its nominal attitude. The attitude control system counteracts these disturbances and maintains the desired attitude. Disturbance torques are either cyclic or secular. Cyclic disturbances do not cause net change in attitude after one complete orbit. Secular torques operate more or less constantly in the same direction; they, therefore, eventually require the operation of thrusters to remove their cumulative effects.

The motion of the spacecraft is measured by attitude sensors and feedback to the controller. There are various types of attitude sensors and actuators (figure 2) and their choice depends on the required attitude accuracy/stability, type of stabilisation used, mission application, reliability and life of the spacecraft.

Attitude control requirements for a given mission depend on application. Important attitude control parameters are: pointing direction, manoeuvres (change in pointing direction), pointing accuracy and stability (maximum attitude rate). Also, it has to meet other mission requirements, such as minimum on-orbit life, reliability, weight and cost.

2.1 *Stabilisation techniques*

A spacecraft that is not stabilised in some way will tumble in orbit due to forces of disturbance present in the space environment. Consequently, payloads, sensors,

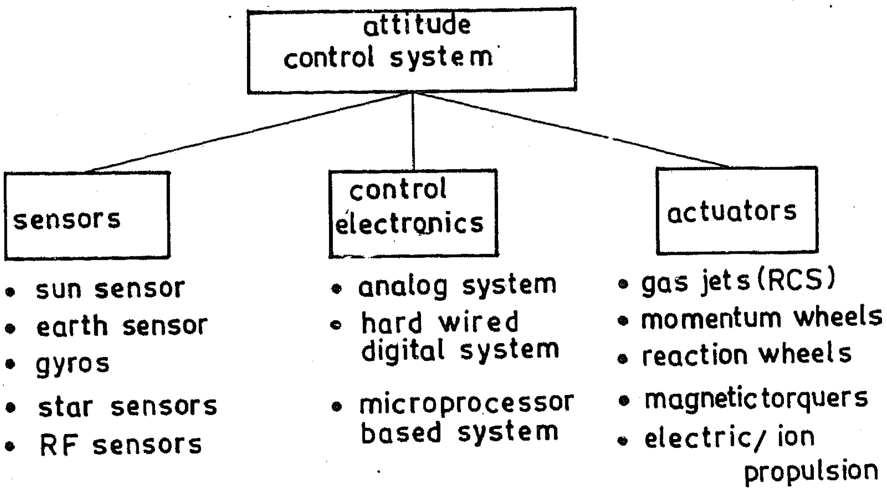


Figure 2. Elements of attitude control systems.

antennae and solar arrays will be pointing in random directions. Spacecraft, therefore, have to be stabilised in orbit to maintain desired orientation.

Spacecraft may be stabilised by passively controlling the axes using environmental torques or by actively controlling the axes using hardware such as gas jets, momentum/ reaction wheels and electro-magnetic torquers. Passive stabilisation makes use of either gravity gradient, solar radiation or aerodynamic environmental torques and does not consume the spacecraft's electrical power and propellants. Also, there is no need for attitude sensors, actuators and on-board controllers. But these techniques have severe limitation on the pointing accuracy and direction of orientation. Further, they depend on the altitude and the shape of spacecraft and are very slow in response. Passive stabilisation techniques are, therefore, not generally used as a primary mode of control. Active stabilisation, on the other hand, is more accurate, flexible and faster; it can be adjusted to meet the mission requirements. In the "zero-g" space environment a small force is sufficient to turn the spacecraft. Spacecraft could be spin stabilised or three-axis stabilised.

2.1a *Spin stabilisation*: The simplest means of controlling the attitude of a spacecraft is to spin the spacecraft about its axis of maximum moment of inertia; the momentum imparted by spin keeps the spin axis fixed in inertial space. Orientation of the spin axis assists the satellite mission to varying degrees. Body-fixed solar arrays in a spinning spacecraft give relatively low solar power – 25 to 30% of sun-oriented solar panel of the same area – since at a time not all the solar cells will be facing the sun. Further, spin stabilisation results in wobble (nutation) and is limited to a single axis.

2.1b *Three-axis stabilisation*: In 'three-axis-stabilisation', also known as body stabilisation, all the three axes, pitch, roll and yaw, are actively controlled using intentionally generated torques to counteract disturbances. In a spacecraft that maintains its orientation relative to earth, i) the yaw axis is directed towards the nadir (i.e. towards the earth centre), ii) the pitch axis is directed towards the negative orbit normal, and iii) the roll axis is perpendicular to the other two such that the unit vectors along the three axes have the relation $\hat{R}=\hat{P}\times\hat{Y}$. The pitch, roll and yaw angles, θ, ϕ and ψ, are defined as right-handed rotations about their axes (Wertz 1978; Thomson 1963).

Stabilisation can be achieved using momentum/reaction wheels, which absorb disturbance torques and mass expulsion devices (such as gas or ion thrusters), and electromagnetic coils, which generate torque by interacting with the earth's magnetic field. A mass expulsion system refers to a reaction control system (RCS) consisting of gas thrusters; it generates force/torque by expelling cold or hot gas under pressure. A very low torque is sufficient to change the orientation of a spacecraft. One pair of thrusters pointing in the opposite directions is provided for each of the three axes and attitude is maintained or altered by 'firing' both the thrusters simultaneously. The thrusters generate short and matched torque pulses. RCS is efficient in execution of a manoeuvre, simple to operate and not limited to a particular altitude/environment. But, they require complex hardware/plumbing and limit the life of the control system by the amount of fuel stored. RCS, however, is essential for recovery from large initial attitude error/rate (attitude acquisition) and for orbit control.

(i) *Momentum biased system*: An internal momentum wheel, a rotating flywheel with a large inertia, is spun up to maintain a large momentum about its spin axis; it keeps that axis stabilised in two coordinates in inertial space. A momentum wheel that is mounted along the pitch axis of a spacecraft actively controls the pitch axis by modulating the wheel speed around a bias speed. Momentum due to disturbance torques are absorbed by momentum wheels. When secular disturbance torques force the wheel speed to go beyond the operating limits, external torquing by a magnetic torquer or by a reaction control system (RCS) is used to bring the wheel speed within limits. This is known as 'momentum dumping'.

Only roll error needs to be corrected, when it exceeds a limit, by external torquing. Roll-yaw coupling, over a quarter of an orbit due to gyroscopic stiffness, automatically limits the yaw error. Pitch and roll errors are sensed by earth sensors. The controller generates control signals for momentum wheels and magnetic torquer/thrusters.

(ii) *Zero momentum (reaction wheel) system*: In a zero-momentum system, spacecraft is stabilized in all the three axes by reaction wheels mounted along each axis. Rotation about any axis is accomplished by changing the speed of the corresponding reaction wheel; no thruster firing is needed until the wheel speed reaches its limits. The nominal speed of a reaction wheel is zero; the wheel can be rotated in either direction to absorb disturbance torques or to reorient the spacecraft. Pitch and roll errors are measured by earth sensors, while the gyro gives the yaw error. An attitude reference system (ARS) using gyros also gives attitude error about all the three axes.

(iii) *Hybrid system*: Stabilisation using the momentum wheels for pitch control and the reaction wheel for roll/yaw control is also feasible. Also two momentum wheels in V-configuration can be used for both pitch and roll/yaw control. Such schemes give continuous pitch and roll control.

(iv) *Magnetic control*: A magnetic field produced by the on-board magnetic coil/torquer interacts with earth's magnetic field and generates torque to orient the spacecraft and to counteract disturbance forces. By controlling magnitude and direction of the current through magnetic torquer, in relation with the earth's magnetic field, the required control torque is obtained.

2.2 *Modes of operation*

Primary modes of operation are: attitude acquisition, attitude maintenance and orbit control. An initial mode of operation, which controls the attitude rates and provides proper orientation after separation from the launcher/booster, is known as attitude acquisition. Attitude maintenance (also known as normal mode) covers operations required to maintain proper attitude/orientation. During this phase, a spacecraft renders the designated services. The other mode·of control ensures proper orientation of the spacecraft during velocity corrections required for orbit control.

The amount of propellant that can be carried becomes the ultimate life-limiting factor of a spacecraft. Lifetimes of upto 10 to 15 years are required in many spacecraft. The possibility of replenishing the propellant while the spacecraft is in orbit by means of excursions by the Space Shuttle promises to remove this limitation; but this is feasible only for low earth-orbiting spacecraft since the Space Shuttle does not reach geosynchronous altitudes.

Also the electromechanical systems that are continuously in rotation, such as momentum/reaction wheels and gyros, must have very long operational life. The reliability, life and criticality of failures determine the number of redundant units and their configuration.

3. Fault-tolerant attitude control system

Fault-tolerant attitude control systems (FACS) consist of a fault-tolerant attitude control electronics and a set of redundant attitude sensors and actuators. The attitude control electronics, besides performing the attitude control function, does the following automatically on board the spacecraft: i) monitors performance of various sensors and actuators, ii) detects and identifies failures, if any, and iii) reconfigures the faulty subsystem. A fault-tolerant attitude control system by tolerating failures in sensors, actuators and control electronics ensures correct operation despite failures; it gives uninterrupted performance and enhances the reliability and probability of mission success.

3.1 *Requirements of* FACS

Essential requirements of a fault-tolerant attitude control system are:

1. Despite single failure in any one or more of the critical subsystems, the attitude control system (ACS) must perform all its functions autonomously and without any interruption. Also, depletion of fuel due to failure should be avoided.
2. The number of redundant units (the degree of redundancy) is to be minimum as there are severe constraints on power consumption, weight, volume and locations used for mounting sensors and actuators.
3. Fault detection, identification and reconfiguration schemes/algorithms should be fairly simple and realisable using a microcomputer.

4. Fault detection and identification schemes, to the extent possible, should be based on the already available performance measures/monitors and other house-keeping information; additional transducers/monitors should be avoided:
5. Transient failures present for relatively short duration and disappearing later, should not result in reconfiguration.
6. FACS should protect against 'hard-over' failures that result in attitude loss, interruption in service and catastrophic effects like depletion of propellant. 'Soft failures' result in marginal degradation in performance and do not cause any catastrophic effects. Soft failures, if any, can therefore be identified by analysing the telemetered data on ground and necessary remedial actions can be taken through telecommand.
7. FACS should store the history of events and information about sequence of actions taken to mask failures and sent them through telemetry.
8. Provision should exist to enable or disable the autonomous reconfiguration, either through telecommand or by signals generated on board.
9. Despite various measures taken if the spacecraft attitude is lost, the fault-tolerance scheme should generate a signal to keep the spacecraft in a 'safe mode', which ensures generation of adequate solar power and healthy, safe and commandable state of the spacecraft. After detailed analysis remedial action can be taken from the ground to resume normal operations, if possible.
10. Add-on approach: Fault-tolerant techniques/schemes should be general in nature so that they are applicable to most spacecraft. Further, fault-tolerance should be achieved with existing and proven subsystems (sensors and actuators) without need for changes/modifications in the sensors and actuators.

3.2 *Fault-tolerance in control electronics*

A fault-tolerant attitude control system requires fault-tolerant control electronics, attitude sensors and actuators (Murugesan 1985). The microprocessor based spacecraft attitude control electronics (microcomputer) and its software can be made fault-tolerant by adopting the well-known hardware and software fault tolerance techniques used for general purpose computers (Avizienis 1976; Anderson & Lee 1981; Hecht 1979; Siewiorek & Swaz 1981; Johnson 1984; Lala 1985). The control electronics, besides performing the functions needed for attitude control, carries out the processing and take decisions ne-essary for fault-tolerance in sensors and actuators (figure 3).

3.3 *Fault-tolerance in sensors*

A traditional scheme for protecting against failures in a sensor is to have three (or more) sensors for measuring the same parameter, with some form of voting on their output. The well-known majority voting, however, is not suited for triplicated sensors since output of different sensors measuring the same parameter may not be exactly equal due to several factors including noise, drift and lack of precision. Therefore, a different selection procedure – such as weighted nonlinear averaging (Brown 1975) and median selection (McConnel & Siewiorek 1981; Ammons 1979), which mask the output that is significantly different from others that are 'nearly alike' – has to be used. This type of voting is known as 'inexact voting'. Weighted non-linear averaging, however, is complex to implement. A simple feedback type

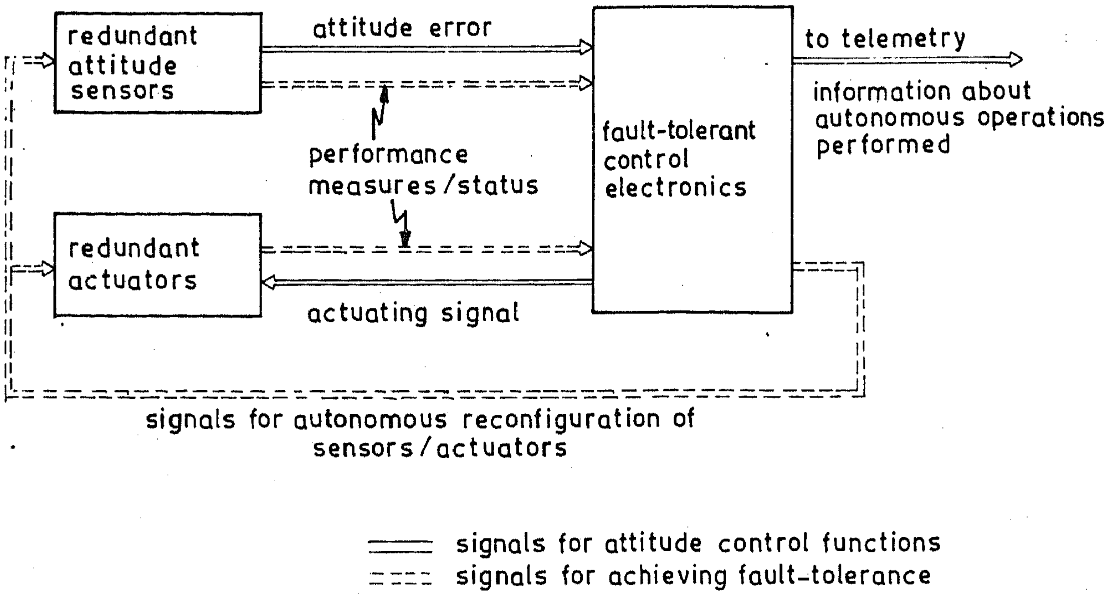

redundant attitude sensors
attitude error
fault-tolerant control electronics
to telemetry
information about autonomous operations performed
performance measures/status
redundant actuators
actuating signal
signals for autonomous reconfiguration of sensors/actuators
signals for attitude control functions
signals for achieving fault-tolerance

Figure 3. Basic scheme of fault-tolerance in attitude control systems.

median selector for analog signals is given in figure 4. A novel and simple cascadable median selector for n-bit digital data using $\lceil n/2 \rceil$ 1K byte PROM (Programmable Read Only Memories) is described by Murugesan (1985).

A static redundant system automatically and instantaneously protects against failures without any need for explicit fault detection and identification of faulty sensor. But this scheme requires three (or more) sensors, imposes a heavy burden on power consumption since all the sensors and its processing electronics are to be powered, and increases the weight, volume, cost and constraints on mounting space/locations for sensors.

In many applications, therefore, a fault-tolerant scheme based on two redundant sensors (dynamic redundancy) is desired. As both the sensors in a dual-redundant system are powered and measure the same parameter, detection of failure, if any, is quite simple. However, there is no direct way of identifying which of the two

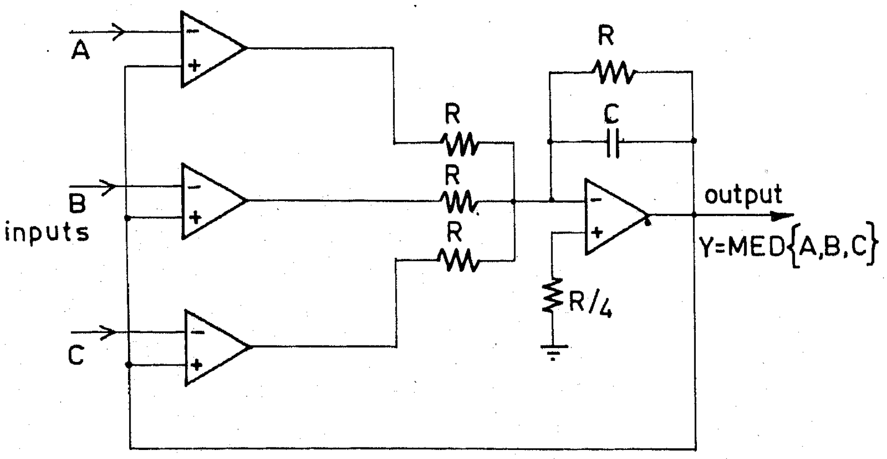


Figure 4. Median selector for analog signals.

sensors is faulty. Many indirect approaches have been proposed for fault detection and identification: Multiple model method (Wilsky 1976), generalised likelihood ratio test (GLRT) (Wilsky 1980), failure detection filters (Wilsky 1976), multiple Luenberger observer (Clark 1975) etc. But these schemes are complex and require a lot of real-time on-board computations. Further, they are sensitive to model errors, system non-linearity and parameter variations. Hence, these techniques are not suitable for on-board implementation in most spacecraft.

Simple fault-tolerance schemes based on the sensor's output and the general behaviour of the spacecraft's attitude are, therefore, developed for earth sensors and given in the next section. Also, a new skewed configuration for a fault-tolerant attitude reference system using three dynamically tuned gyros (DTG) is described in §5. It is an optimum configuration in terms of error in the attitude estimate, computational requirements/complexity and fault coverage. This configuration is better than the other configurations proposed so far.

3.4 *Fault-tolerance in actuators*

The nature of failures in actuators and their effects is different from that of sensors and computers. Fault-tolerance schemes suitable for sensors/computers, therefore, may not be directly suitable for actuators. For instance, an actuator that failed in a continuous actuating mode can·not be simply substituted by a redundant actuator, leaving the faulty actuator as such, as is usually done in sensor/computers. The failed actuator is to be prevented from having any further effects on the overall system performance, and leaky or fully open flow control valves/pipe lines have to be inhibited before an alternate valve/path is chosen and depletion of propellant/fuel has to be stopped. The fault-tolerance approach differs depending on the type of actuator.

Failure modes and fault detection and identification (FDI) algorithms for reaction/momentum wheels and reaction control systems (RCS) are described in the subsequent sections. The control electronics monitor the performance of actuators, detect and identify the failure based on the FDI algorithms (developed in this work) and reconfigure the actuators accordingly.

4. Fault-tolerant dual-redundant earth sensor

Earth sensors measure both pitch and roll errors of a three-axis stabilised satellite. They basically detect the infrared radiation from earth and compute pitch and roll errors, θ and ϕ, respectively. The outputs of earth sensors (ES) are fed to controllers; the controllers drive the actuators so as to correct the attitude errors, if any, and maintain the spacecraft in the desired orientation. Two earth sensors ES_1 and ES_2 are used, as shown in figure 5, which are redundant to each other. Outputs of either of the sensors can be selected for closed-loop attitude control. The two earth sensors may be identical or of different types, thereby providing 'design diversity'.

Earth sensor failures can broadly be classified as soft and hard failures. Bias errors, excessive random noise on output and scale factor errors are considered as soft failures. Under hard failures, however, outputs may be stuck-at-a-low value,

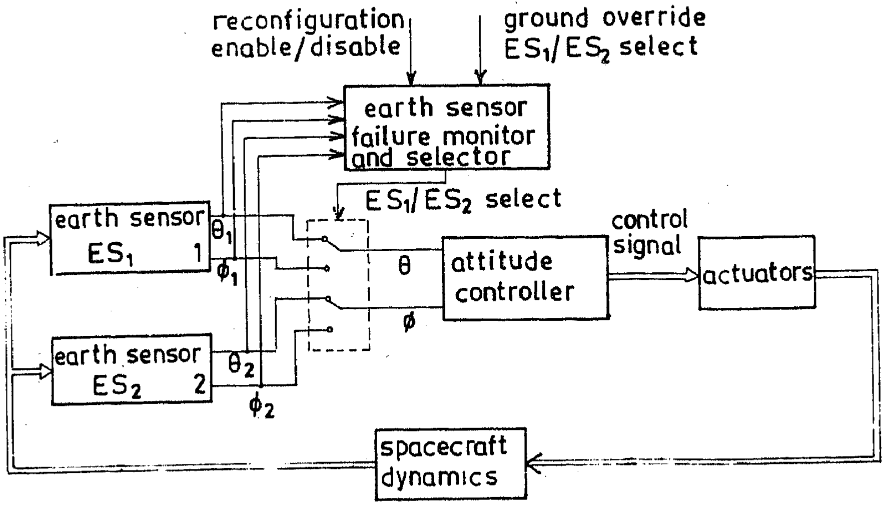


Figure 5. Fault-tolerant dual-redundant earth sensors.

including zero, or stuck-at-a-higher value (relative to normal attitude error), including saturated levels. While soft failures result in poor measurement accuracy and hence degraded performance of the attitude control system, hard failures lead to attitude loss and might jeopardize the whole mission. Thus, hard failures are more critical than soft failures.

4.1 *Detection and identification of failures*

When both the sensors ES_1 and ES_2 measure attitude of the spacecraft, performance of a sensor can be compared with respect to the other, facilitating easy detection and identification of certain sensor failures. For instance, if only one sensor is working and measured attitude error shows an unusually high value, we cannot conclude that error is high because of failure of the sensor, since failure of the controller and/or actuators also could result in higher attitude errors. Thus, it is very difficult to identify the exact source of failure in a closed-loop control system without additional information.

In an ideal situation, outputs of both the sensors would be exactly equal and hence their difference would be zero. However, because of non-identical sensing, misalignment, unequal bias, minor variations in scale factors and random noise, a non-zero difference is normally obtained even if both the sensors are working properly.

Either ES_1 or ES_2 can be selected for closed-loop attitude control; the sensor in the loop is designated as ES_A, while the other that is not used for closed-loop control is designated as ES_B. Considering the possibility of hard failures in one of the sensors of a dual-redundant sensor system, the five operating conditions are as in table 1.

An algorithm for detection and identification of hard failures of earth sensors is given in figure 6. When an output of the sensor ES_A, which in the closed-loop, fails at high, controllers would be continuously torquing the reaction/momentum wheels and/or thrusters in the same direction resulting in continuous increase in attitude errors in the opposite direction. The attitude errors, however, would be properly sensed by the redundant sensor ES_B, which is not in the loop. If the difference in

Table 1. The five possible operating conditions of a dual-redundant sensor system

Sensor in the loop ES_A	Sensor not in the loop ES_B
Ok	Ok
Stuck-at-high	Ok
Stuck-at-low	Ok
Ok	Stuck-at-high
Ok	Stuck-at-low

pitch or roll outputs of two sensors ES_A and ES_B, $(\theta_A-\theta_B)$ or $(\phi_A-\phi_B)$,exceeds the threshold e_d indicating failure of one of the sensors, and if the outputs θ_A or ϕ_A are greater than the upper limit e_U for at least three consecutive samples, then ES_A is considered faulty.

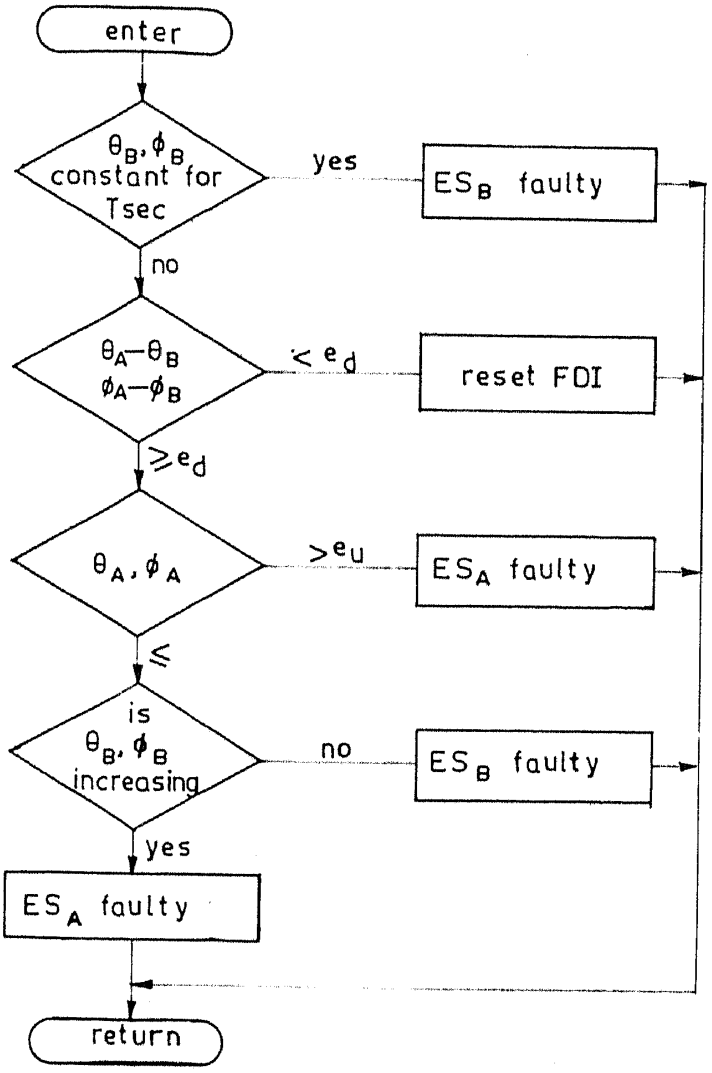


Figure 6. FDI algorithm for dual-redundant earth sensor.

On the other hand, if the sensor ES_A is stuck at zero (or low), the controller output will be near zero and hence the actuators will not impart significant torque to the spacecraft. Since attitude is not controlled under this failure mode, attitude error would gradually build up depending on residual rate and disturbance on the spacecraft. But the attitude error will be properly measured by ES_B. Thus, when the difference in the outputs of the sensors ES_A and ES_B exceeds the threshold, e_d, failure will be detected. If the attitude error as measured by ES_B still continues to increase in the same direction, the sensor ES_A is considered stuck-at-low.

If the failure of earth sensor is detected and the above checks do not indicate failure in ES_A, even after an elapse of sufficiently large time (about 100s or so), then $\mathrm{ES}_B$is considered faulty. Stuck-at-zero (low) failures in ES_B, do not have any impact on the spacecraft performance or on the other sensors, and hence, it can not be identified by the above methods. If a sensor is functioning normally, there would be small variations (noise) in the output. However, if an output is stuck-at-zero or any other value, there would not be any change/variations. Thus, if the output θ_B or ϕ_B remain constant without any changes for a large duration (100s) then ES_B is considered faulty.

Excessive random noise in sensor outputs is detected using the statistical technique 'hypothesis testing' Variance of a set of samples of an output is a measure of scatter of the output about the mean value; if it exceeds an upper limit that output is excessively noisy, and hence, the sensor is considered faulty. 'Trend' in output has, however, to be removed before computation of sample variance

Although bias errors are less troublesome, if its magnitude is high it will shift the orientation of the spacecraft, and hence the payload, resulting in performance degradation and/or interruption in service. Let us assume that sensor ES_A which is in the closed-loop has developed a bias error of $+\theta_b$. Because of closed-loop control action, the output ES_A will be maintained near zero by orienting the spacecraft towards the opposite direction, resulting in attitude error of $-\theta_b$. As the redundant sensor ES_B (which is not in the loop) is functioning properly, its output will correctly measure the attitude error of $-\theta_b$. On the other hand, if ES_A is functioning properly and ES_B has a bias of $-\theta_b$, then also the output of ES_Awould be near zero, while that of ES_B would be $-\theta_b$. Bias errors of sensors used for closed-loop control, therefore, cannot be directly detected and identified from the sensor outputs alone and an indirect approach using other factors which depend on the type of attitude stabilisation and controller used is required. As the scheme is not general and is mission-specific, it is not described further here. Further details are given elsewhere (Murugesan 1985).

4.2 *Autonomous reconfiguration of earth sensors*

The reconfiguration scheme for earth sensors is as follows:

(i) If ES_1 outputs are being used for closed-loop control and the sensor is found faulty, the outputs of the redundant sensor ES_2 are selected for closed-loop control; on the other hand, if ES_2 has failed, ES_1 outputs continue to be used for control.
(ii) If ES_2 outputs are being used for closed-loop control and ES_2 is found faulty, the outputs of ES_1 are selected for closed-loop control; on the other hand, if ES_1 is faulty, ES_2 outputs continue to be used for closed-loop control.

The above scheme for sensor failure detection is insensitive to failures in other subsystems. For instance, if attitude errors become large due to improper functioning of attitude control electronics or actuators, the earth sensor will not be identified as faulty since outputs from both the sensors would still be nearly equal, indicating proper operation of both the sensors. Further, although fault detection time is high under certain failure modes, it does not significantly affect the performance of a spacecraft, as the time constant of a spacecraft attitude control system is high.

5. Fault-tolerant attitude reference system using dynamically tuned gyros

Attitude reference systems (ARS) using gyros give the attitude of a spacecraft about the three orthogonal reference axes X_1, X_2 and X_3; they are preferred for spacecraft control applications since they have better (short-term) accuracy than earth sensors. For achieving very high reliability over a long period and for fault-tolerance, attitude reference systems use more gyros than the minimum required for basic measurement along the three principal axes. Fault-tolerance is achieved by autonomous failure detection and identification (FDI) and isolation of a faulty gyro, with subsequent modification in attitude estimation schemes. Also, redundant information improves accuracy of the derived attitude estimate by reducing uncertainties.

A dynamically tuned gyro (DTG) measures angular information along two perpendicular directions and two DTG are sufficient to provide attitude information about all the three axes. But, an ARS using more than two DTG provides attitude information about all the three principle axes despite failure of one or more DTG. An attitude reference system with three DTG can tolerate failure of any one DTG.

DTG can be arranged in various geometrical configurations. The basic considerations involved in selecting a particular configuration are: (1) effectiveness of fault detection, identification and reconfiguration, (2) simplicity of computations and processing, and (3) error in estimated attitude for a given error in gyro output.

The orthogonal configuration (Harrison & Chen 1975) has the measurement axes of DTG along the reference axes. It is simple and gives minimum error in the estimated attitude, for a given error in gyro output. Though the orthogonal configuration is claimed to be the optimum configuration, identification of faulty DTG is based on the hypothesis that if a DTG fails then its outputs from both the axes will be erroneous. However, when failure is not common to both the axes, a particular output alone would be erroneous, while the other output is correct. For instance, if final output-buffer, parallel-to-serial shift register or a logic gate of an output is faulty, then that output alone would be erroneous. Hence, in the orthogonal configuration one cannot identify and tolerate a faulty DTG under all types of failure.

Though orthogonal-cum-skewed (Engelder 1980) and coplanar (Harrison & Gai 1977) configurations tolerate all modes of failure of DTG, they give more error in the attitude estimate than the orthogonal scheme. Further, processing and FDI schemes for these configurations involve more computations.

We, therefore, have developed a new symmetrically-skewed optimum configuration for an attitude reference system using three DTG (figure 7). Three DTG D_1, D_2, and D_3 are arranged such that,

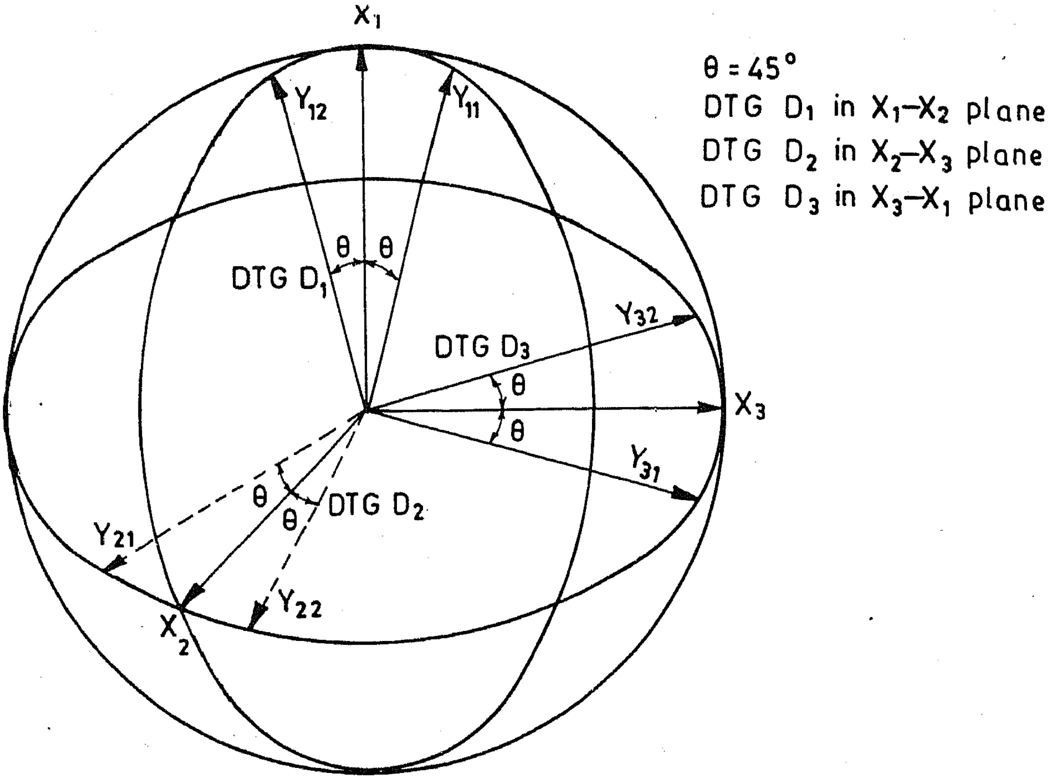


Figure 7. A new symmetrically skewed configuration for the attitude reference system using DTG.

(i) the measurement axes Y_{11} and Y_{12} of DTG D_I lie in the X_1-X_2 plane and make an angle of 45° with respect to the reference axis X_1.
(ii) the measurement axes Y_{21} and Y_{22} of DTG D_2 lie in the X_2-X_3 plane and make an angle of 45° with respect to the reference axes X_2, and
(iii) the measurement axes Y_{31} and Y_{32} of DTG D_3 lie in the X_3-X_1 plane and make an angle of 45° with respect to the reference axis X_3.

The outputs y_{ij}, i=1 to 3 and j=1 to 2 from the DTG are related to the attitude x_1, x_2 and x_3 along the three principal axes as follows:

$$\begin{bmatrix} y_{11} \\ y_{12} \\ y_{21} \\ y_{22} \\ y_{31} \\ y_{32} \end{bmatrix} = \begin{bmatrix} C & -C & 0 \\ C & C & 0 \\ 0 & C & -C \\ 0 & C & C \\ -C & 0 & C \\ C & 0 & C \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \xi, \tag{1}$$

where $C = 0{\cdot}7072$ and ξ is the measurement noise.

Attitude estimates $\hat{x}_1$, $\hat{x}_2$ and $\hat{x}_3$ are obtained from the output of DTG y_{ij}, $i = 1$ to 3, $j = 1$ to 2, using the least square estimation technique. The attitude estimate when all DTG are functioning properly is given by

$$\hat{x}_1 = K_3(y_{11}+y_{12}-y_{31}+y_{32}),$$
$$\hat{x}_2 = K_3(y_{21}+y_{22}-y_{11}+y_{12}),$$

$$\hat{x}_3 = K_3(y_{31}+y_{32}-y_{21}+y_{22}), \tag{2}$$

where $K_3 = 0{\cdot}3536$.

5.1 *Failure detection, identification and reconfiguration*

For detection and identification of faulty DTG, however, a set of parity equations $\{p_1, p_2 \dots p_k\}$ is required. A parity equation is a linear combination of the DTG output, y_{ij}, and is independent of the attitude x_1, x_2 and x_3 along the three reference axes. The parity equation is defined as

$$p = f\,(y_{11}, y_{12}, y_{21}, \dots y_{N1}, y_{N2}),$$

and by definition,

$$p \neq f\,(x_1, x_2, x_3). \tag{3}$$

Thus, parity equations expose only the combined measurement error, if any, and not attitude information.

The set of parity equations, however, must satisfy the following conditions: (1) each measurement is incorporated in at least one parity equation, and (2) the pattern of parity equations should provide the information necessary for fault identification. The parity equations are given by

$$\begin{aligned} p_1 &= (y_{11}+y_{12})+(y_{31}-y_{32}),\\ p_2 &= (y_{21}+y_{22})+(y_{11}-y_{12}),\\ p_3 &= (y_{31}+y_{32})+(y_{21}-y_{22}). \end{aligned} \tag{4}$$

Under failure-free operation of the DTG, the three parity equation residuals p_1, p_2 and p_3 would be very low. But, if a DTG is faulty, and hence any one or both of its outputs are erroneous, then those parity equation residuals involving the erroneous output will have a large value. To detect failure in a system, therefore, the parity equation residuals are compared with a failure threshold, f_{th}, selected in consistency with normal measurement errors, uncertainties and noise.

The Boolean variable F_i is set to ONE if the parity equation residual p_i is greater than f_{th}; and reset to ZERO otherwise; i.e.,

$$\begin{aligned} F_i &= 1, \quad \text{if} \quad p_i > f_{\text{th}},\\ &= 0, \quad \text{otherwise}, \quad \text{for } i = 1 \text{ to } 3. \end{aligned} \tag{5}$$

In case of failure of a DTG, two of the three Boolean variables F_1, F_2 and F_3 would be ONE, thereby detecting a failure in the attitude reference system.

The value of the Boolean variable F_i can also be decided based on current and the last few observations using statistical techniques such as the Generalised Likelihood Ratio Test (GLRT) (Daly *et al* 1979) and modified sequential probability ratio test (Chin & Adams 1976). The advantage of these techniques is that even the smallest failure magnitudes falling within the range of measurement uncertainties and noise can be detected with low probabilities of false and miss alarm. But these schemes require additional computations/processing.

A faulty gyro can easily be identified from the Boolean variables F_1, F_2 and F_3. For instance, if the DTG D_1 is faulty, and either one or both of its outputs y_{11} and y_{12} are erroneous, then the parity equation residuals p_1 and p_2 will exceed the failure threshold f_{th} setting F_1 and F_2 to ONE. Since the outputs of the other DTG are correct, the parity equation residual p_3 will be less than the threshold and, hence, F_3 will be ZERO. Thus, if F_1 and F_2 are ONE and F_3 is ZERO, DTG D_1 is faulty. Similarly, other faulty DTG can be identified from F_1, F_2 and F_3.

The DTG D_i is faulty if the Boolean variable L_i as given below in (6), is ONE; otherwise the DTG D_i is faulty-free.

$$\begin{aligned} L_1 &= F_1 \quad F_2 \quad \bar{F}_3, \\ L_2 &= \bar{F}_1 \quad F_2 \quad F_3, \\ L_3 &= F_1 \quad \bar{F}_2 \quad F_3. \end{aligned} \tag{6}$$

As seen from parity (4) and the Boolean equations (6) for fault identification, this FDI scheme detects and identifies a faulty gyro irrespective of whether one or both the outputs of the DTG are erroneous.

When a DTG is faulty, the attitude along the three principle axes is estimated from the outputs of the other two DTG, based on the least square estimation technique, ignoring both the outputs of the faulty DTG. The attitude estimates for various cases of failure of DTG are given in figure 8.

The proposed configuration is better than the other configurations and requires only simple computations for estimation of attitude and fault detection and identification (FDI). It tolerates failure in one or both the outputs of a DTG and gives the same accuracy in the attitude estimate as that of the orthogonal configuration. Comparison of various configurations is given in Murugesan (1985).

6. Fault-tolerant reaction/momentum wheel system

A reaction wheel basically consists of a flywheel (disc-shaped rotating mass of required inertia) driven by an electric motor and the associated bearings and drive electronics. The reaction wheel rotates in either direction from zero to a maximum permissible speed of about 6000 rpm. For long-life operation iŋ space, conventional brushed d.c. motors are not suitable as drives for reaction/momentum wheels due to severe catastrophic wear of brushes and commutator segments, possibility of 'cold welding' between contacting surfaces under hard vacuum and arcing across brushes and commutating segments. Iron-less brushless d.c. motors are, therefore, generally used for reaction/momentum wheels.

Another critical component in the reaction/momentum wheel is the bearing; it should withstand over ten years of continuous operation. Further, conventional lubrication is not adequate for space applications. Hence, specially designed and lubricated ball-bearings with better finish of balls and races are used. With advances in magnetic materials and microelectronics, magnetic bearings that do not have physical contact between rotor and stator are being increasingly used in reaction/momentum wheels. Magnetic bearings facilitate higher wheel speeds and enhance operation life of reaction/momentum wheels.

Reaction torque: The change in wheel speed gives rise to reaction torque, and hence, counters disturbance torques about the axis of angular momentum vector. The reaction torque, T_R, is given by

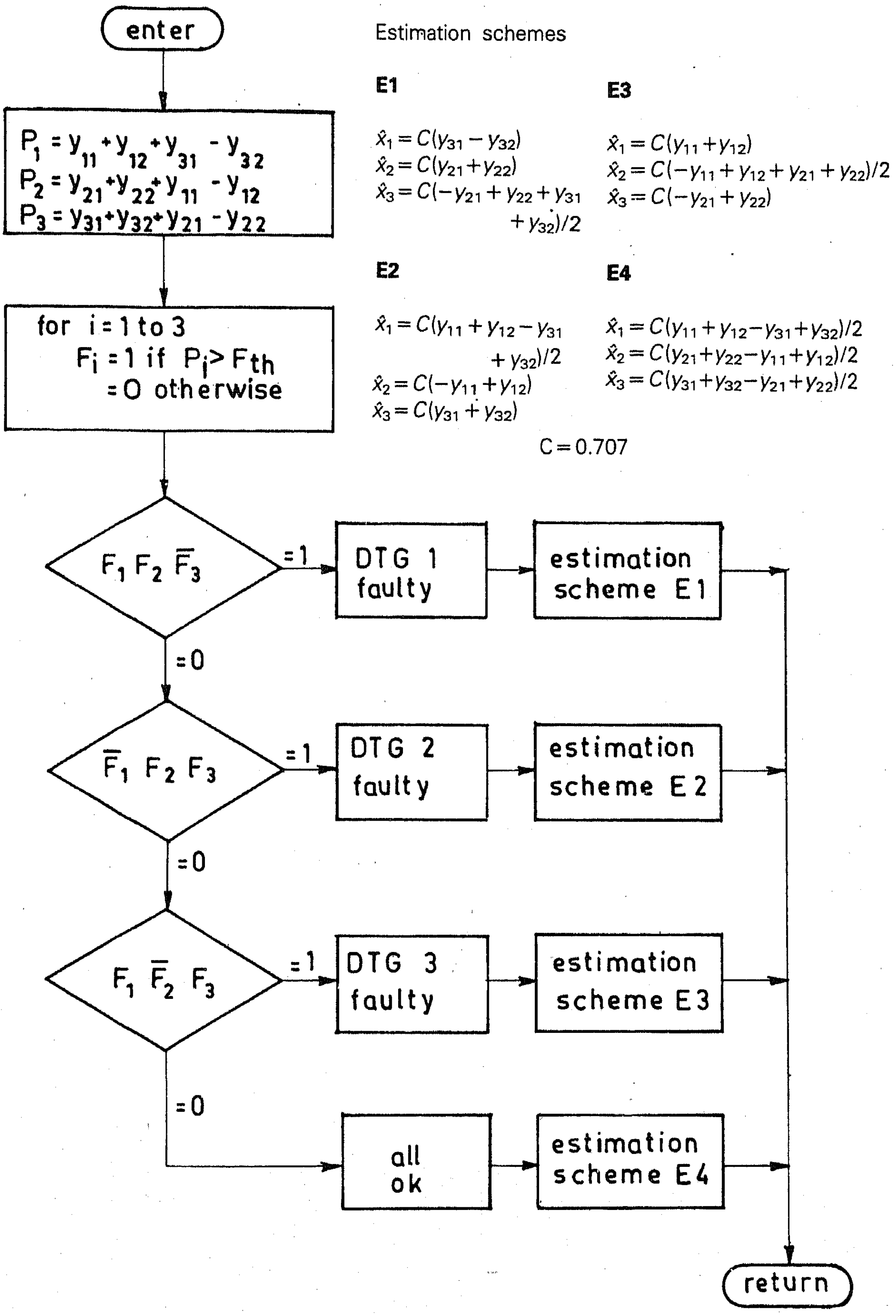

enter
$P_1 = y_{11} + y_{12} + y_{31} - y_{32}$
$P_2 = y_{21} + y_{22} + y_{11} - y_{12}$
$P_3 = y_{31} + y_{32} + y_{21} - y_{22}$
for $i = 1$ to 3
$F_i = 1$ if $P_i > F_{th}$
$= 0$ otherwise
Estimation schemes
E1
$\hat{x}_1 = C(y_{31} - y_{32})$
$\hat{x}_2 = C(y_{21} + y_{22})$
$\hat{x}_3 = C(-y_{21} + y_{22} + y_{31} + y_{32})/2$
E3
$\hat{x}_1 = C(y_{11} + y_{12})$
$\hat{x}_2 = C(-y_{11} + y_{12} + y_{21} + y_{22})/2$
$\hat{x}_3 = C(-y_{21} + y_{22})$
E2
$\hat{x}_1 = C(y_{11} + y_{12} - y_{31} + y_{32})/2$
$\hat{x}_2 = C(-y_{11} + y_{12})$
$\hat{x}_3 = C(y_{31} + y_{32})$
E4
$\hat{x}_1 = C(y_{11} + y_{12} - y_{31} + y_{32})/2$
$\hat{x}_2 = C(y_{21} + y_{22} - y_{11} + y_{12})/2$
$\hat{x}_3 = C(y_{31} + y_{32} - y_{21} + y_{22})/2$
$C = 0.707$
$F_1 F_2 \bar{F}_3$
=1
DTG 1 faulty
estimation scheme E1
=0
$\bar{F}_1 F_2 F_3$
=1
DTG 2 faulty
estimation scheme E2
=0
$F_1 \bar{F}_2 F_3$
=1
DTG 3 faulty
estimation scheme E3
=0
all ok
estimation scheme E4
return

Figure 8. FDI algorithm for attitude reference systems.

$$T_R = I(dS/dt), \tag{7}$$

where S = wheel speed, rad/s; and I = moment of inertia of the wheel, kg.m^2. Depending on the control signal from attitude control electronics, the reaction/momentum wheel varies its speed, thereby generating the required reaction torque.

The reaction wheel operates over a nominal speed of zero. When the wheel speed reaches its maximum limit in either direction due to accumulated corrections of secular disturbance torques, the wheel speed is brought within the limits by imparting external torque using thrusters or a magnetic torquer.

Momentum wheels are similar to reaction wheels in principle of operation except that a momentum wheel operates only in one direction over a large bias speed (also known as nominal speed) of about 3000 to 6000 rpm.

6.1 *Failure modes and their effects*

Reaction/momentum wheels might fail in one or more of the following modes.

1. *Failure to respond to control signals*: This type of failure causes the wheel to decelerate slowly or hold its speed, without any response to control signals. Faulty commutation/drive electronics, drive motor and power supply, break in the interconnecting wires and grounding of the electrical inputs/outputs might result in this type of failures.

2. *Decreased reaction torque*: Due to increased friction between stator and rotor, inadequate lubrication and marginal failures in bearings and its races, and decreased motor torque and current drive, for a given torque control signal, the rate of change of speed, and hence, generated reaction torque, might be less than the nominal value.

3. *Increased bias torque*: When the torque control signal (TCS) is zero the wheel should hold its speed thereby generating no reaction torque. But, because of changes in the friction due to aging, temperature etc., the wheel may not be able to hold its speed. The speed may either increase or decrease gradually, thereby generating a low reaction torque, known as bias torque, even when the TCS is zero.

4. *Continuous generation of reaction torque*: Stuck-up failures in commutation/drive electronics might result in continuous increase or decrease in speed, thereby generating reaction torque, independent of the torque control signal.

5. *Excessive noise torque*: A major source of torque noise is bearings. Wear or deformation of certain balls in the bearings, increased gap between the bearing and its races, or cage instability give rise to non-uniform movement of the rotor/wheel at certain locations during a revolution. As reaction torque is proportional to instantaneous rate of change of the speed, any non-uniformity in the movement results in torque noise. It is generally random in nature. Also, due to commutation at low speeds, the torque generated by d.c. motors might have some torque ripple/noise.

All these failures except excessive torque noise might result in large attitude errors and/or attitude loss. The consequences of these failures range from interruption in service for a few days and difficult reacquisition of attitude to catastrophic ending of the mission.

Excessive torque noise from a reaction/momentum wheel results in increased jitter, without significantly affecting attitude error. Attitude errors remain within the normal limits even with excessive torque noise. While increased jitter does not affect the services rendered by geostationary communication satellites, it might result in poor quality of pictures and/or data obtained from remote sensing and meteorological satellites. Jitter cannot easily be measured on board a spacecraft. In view of the noncritical nature of this failure and the complexity in measurement of jitter/torque noise, it is not necessary to protect automatically the reaction/momentum wheel system against excessive torque noise. Corrective actions, if necessary, could be taken from the ground itself without major shortcomings, by switching over to redundant wheels through telecommands.

6.2 *Fault detection and identification*

The fault detection and identification algorithm for reaction/momentum wheels should detect and identify the wheel failures alone; faults in other subsystems should not be misinterpreted as faults in reaction/momentum wheels. Further, it is desirable that the algorithm is based on the already existing measurements/parameters.

The 'failure sensitive filter' proposed by Marie (1982) is complex and can detect only abrupt and hard failures of the wheels. We, therefore, develop here a simple FDI algorithm (Murugesan 1981, 1984a to detect all types of wheel failures except the excessive torque noise which anyway does not result in catastrophic effect or interruption in service.

All types of failures of a reaction/momentum wheel directly affect change in wheel speed and hence the reaction torque. For instance, in the case of no response to the torque control signal (TCS), the wheel speed might remain the same or decelerate slowly due to natural run-down independent of the TCS; reduced reaction torque is due to reduced rate of change of wheel speed; bias torque results in continuous change in wheel speed even when the TCS is zero. Change in wheel speed is, therefore, taken as the basis for detection and identification of a faulty wheel.

The FDI algorithm (figure 9) is based on comparison of actual and expected changes in wheel speed during a given duration for a given torque control signal.

The expected change in wheel speed of an ideal failure-free wheel, S_e, over an interval t_m is computed by integrating the torque control signal as given below:

$$\Delta S_e = (G/I) \int_{t_1}^{t_1+t_m} T_s \mathrm{d}t \tag{8}$$

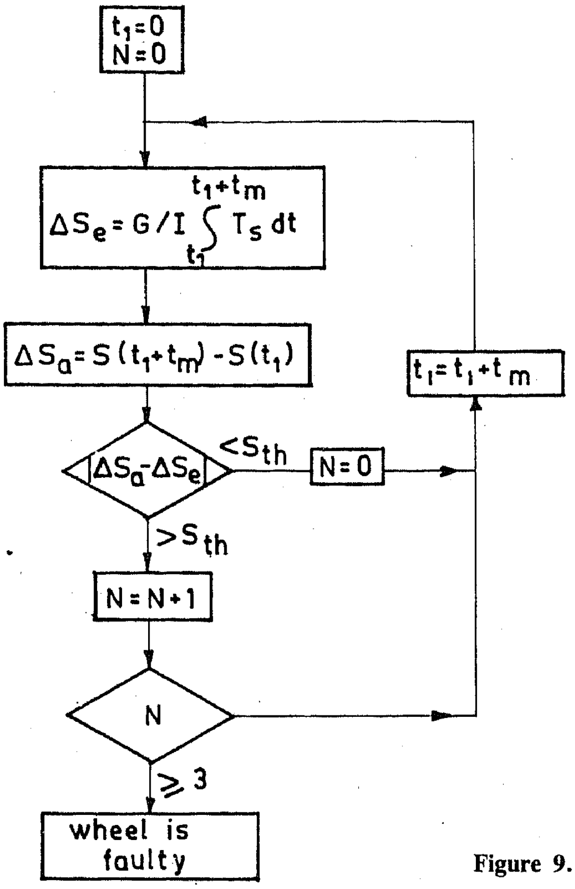
where, I = moment of inertia of the wheel, kg.m^2; T_s = torque control signal, volts; G = gain factor, Newton-metre/volt.

Actual change in wheel speed, over the same interval,

$$\Delta S_a = S(t_1+t_m) - S(t_1), \tag{9}$$

where, $S(t_1+t_m)$ is wheel speed at $t = t_1+t_m$; $S(t_1)$ is the wheel speed at $t = t_1$.

For a properly functioning and fault-free wheel, actual and expected changes in wheel speed during a given interval would nearly be the same; there may, however, be some difference between these two changes in speed because of non-zero bias torque, variations in gain factor due to aging, temperature etc., and uncertainties



$t_1 = 0$
$N = 0$
$\Delta S_e = G/I \int_{t_1}^{t_1+t_m} T_s \, dt$
$\Delta S_a = S(t_1+t_m) - S(t_1)$
$|\Delta S_a - \Delta S_e|$
$<S_{th}$
$N = 0$
$>S_{th}$
$N = N+1$
N
≥ 3
wheel is faulty
$t_1 = t_1 + t_m$

Figure 9. FDI algorithm for reaction/momentum wheels.

and errors in speed measurement. A certain number of these variations/ imperfections are acceptable as they do not significantly affect spacecraft attitude. A faulty wheel, however, will result in a large difference between these two changes in speed. Therefore, for detection and identification of a faulty wheel, the magnitude of the difference between the actual and expected changes in speed of a wheel is compared with a threshold.

If the difference between the actual and expected change in wheel speed of a reaction/momentum wheel is more than the threshold for at least three or more consecutive measurements, then that particular wheel is considered faulty. Check for consistency in fault identification for three consecutive measurements gives protection against transient malfunction of the wheel and spurious speed information.

6.3 *Reconfiguration and recovery*

If a reaction/momentum wheel is identified as faulty, then that particular wheel is switched off and a redundant wheel is enabled automatically to perform the function of the faulty wheel, with necessary modifications/changes in the controllers. Recovery from failures and resumption of normal performance is accomplished by the redundant wheel.

The faulty wheel that is switched off will decelerate very slowly because of its friction (natural run-down) giving very small disturbance torque to the spacecraft. The run-down may even continue for one or two hours if the wheel has been running near the maximum operating speed. However, this disturbance torque will be absorbed by the redundant wheel since its torquing capability is much higher than the disturbance torque generated during natural run-down.

Although the fault detection and identification algorithm remains the same for various geometric arrangements of reaction/momentum wheels, the exact reconfiguration scheme varies depending on the physical arrangement and number of wheels. Further details are given in Murugesan (1981, 1985).

7. Fault tolerance in the reaction control system

A reaction control system (RCS) basically consists of a propellant tank, to store required propellant at high pressure, an electrically operated isolation valve and a set of thrusters in different physical locations on the spacecraft to generate required thrust and/or torque about a desired axis. Isolation valves are used to either block or allow the flow of propellant from storage tank to thrusters, by energising appropriate electromagnetic coils of the isolation valves. A thruster consists of a flow control valve (FCV) and a combustion chamber. When propellant passes through the combustion chamber, chemical reaction takes place generating a thrust through the nozzle. However, when FCV is not energised, the propellant flow to the combustion chamber is inhibited and hence, thrust is not developed.

A reaction control system is used during various phases of a mission for attitude control during transfer orbit, spacecraft attitude acquisition, orbit correction (station-keeping) and momentum dumping operations. It uses stored propellant (fuel) for generation of thrust/torque, unlike the other actuators like reaction/ momentum wheels and magnetic torquers which make use of on-board generated solar power. Operation of RCS consumes propellants, thereby depleting the propellant available for further use. When propellant is completely depleted, RCS cannot generate any thrust eventually ending the useful life of the mission. Proper operation of RCS, without any additional depletion of propellant due to faults in the system is, therefore, essential for the success of a spacecraft mission.

To avoid single point failures, generally, RCS has two sets of functionally redundant thrusters, a set of isolation valves and two propellant tanks (figure 10). Upon actuating signal from the attitude controller, thrusters develop the needed thrust/torque. Any one or both the blocks (block 1 and 2) can be enabled or disabled through ground commands.

7.1 *Failures in RCS and their effects*

In a reaction control system the critical and most probable source of failure is the thruster (flow control valve). Certain types of failures in RCS, apart from resulting in loss of spacecraft attitude, might completely deplete the propellant before any corrective action could be taken from the ground through telecommands.

The large thrust developed by faulty thrusters, that are stuck-at-open or have a large leakage, cannot be compensated by reaction/momentum wheels used for attitude control during the normal phase of a mission. Eventually, these types of

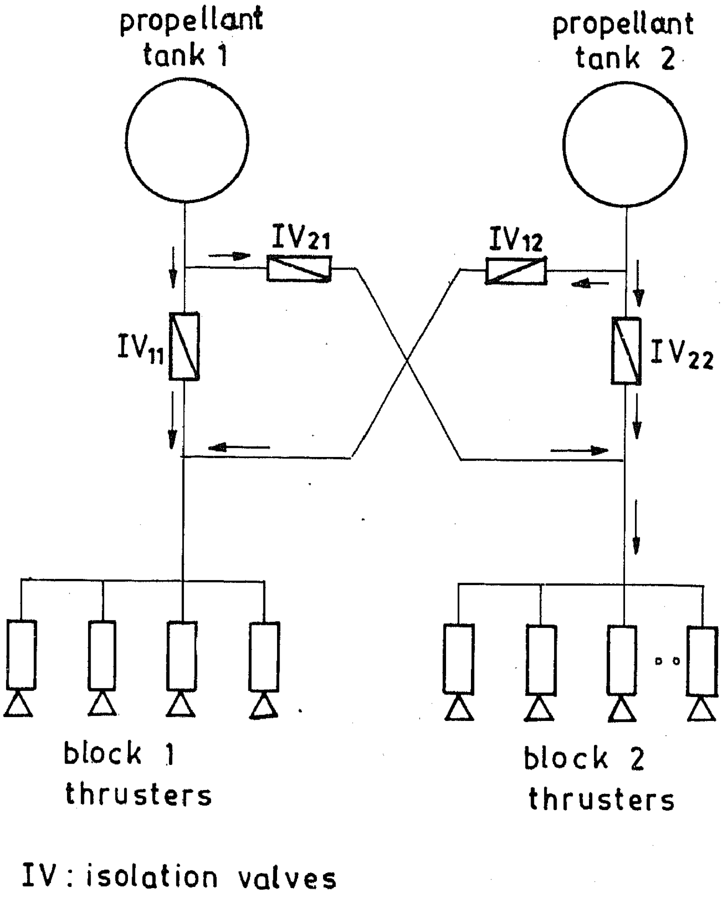


Figure 10. Schematic of a typical reaction control system.

failures, if not corrected, result in rapid attitude error build-up and hence lead to loss of attitude, and more importantly, deplete the propellant, reducing the mission life and/or terminating the mission.

Failures resulting in low leakage give continuous low-level thrust or torque, which can be compensated by reaction/momentum wheels used for the normal phase of operation. But, there would be more frequent momentum dumpings, due to excessive wheel speed build-up. Though small leakages may not result in appreciable attitude error, considerable amount of propellant may be depleted reducing the life of the mission.

A stuck-at-close mode failure, however, does not generate disturbance torques, deplete the propellant or directly result in catastrophic effects. But, such a faulty thruster does not generate thrust/torque when required, and hence, ceases to perform its function of effectively correcting attitude errors and reducing the wheel speed when momentum dumping is carried out.

7.2 *Fault detection*

Detection and identification of a faulty thruster would have been quite simple if the actual thrust developed by each thruster is directly measured. Incorporation of transducers for thrust measurement is complex and adds to failure modes and unreliability. Detection and identification of faulty thrusters has, therefore, to be based on indirect information such as overall attitude performance of the spacecraft.

Stuck-at-open and large leakage failures result in rapid attitude error build-up and large attitude errors, and finally lead to loss of attitude. Fault detection based on attitude error rate alone, however, could be misleading and result in wrong interpretation, since attitude error rates could vary considerably during normal operation itself; for instance, between zero crossing and peak of the attitude errors that vary between positive and negative values in a limit cycle, and sudden external disturbances. On the other hand, a decision based on absolute error alone also could mislead, since excessive bias torque in reaction/momentum wheel results in large attitude error. These types of failures are, therefore, detected by comparing the rate of attitude error build-up and the absolute value of the attitude error with their upper limits.

Low-level leakage of propellant gives a low bias thrust/torque. These disturbances can be counteracted by reaction/momentum wheels and/or thrusters and the controllers used for normal phase operations. Therefore, there may not be appreciable increase in attitude errors and their rate. Hence, these failures are detected based on on-board comparison of the 'behaviour' of controllers with the 'behaviour' during failure-free operation.

In a reaction-wheel-based control system, wherein reaction wheels are used for attitude control along all the three axes of a spacecraft, the disturbances due to low-level leakage lead to excessive wheel speed build-up since the wheels counteract these additional disturbances also. Hence, more frequent momentum dumpings than is needed during the normal failure-free operation would take place. Therefore, fault detection is based on the number of momentum dumping operations performed during a given duration. Though the detection time may be relatively large, it does not significantly affect the system performance and propellant depleted due to low-level leakage might not be much.

In a momentum wheel system, by monitoring excessive momentum dumpings and roll corrections by thrusters over a given duration, low-level leakages in RCS are detected. In a hybrid system also low-level leakages in thrusters are detected by comparing the number of momentum dumping operations about pitch and roll axes for a given duration, with a threshold.

Thrusters failing at the stuck-at-closed mode do not generate torque/thrust when required and hence controllers will not be able to effectively correct the attitude errors and reduce the wheel speed when the momentum dumping operation is carried out. Consequently attitude errors and wheel speed will exceed the normal limits. Thus, when sensors and control electronics are working properly, but attitude error and/or wheel speed corresponding to that function go beyond the normal limits, the reaction control system is considered faulty.

7.3 *Fault identification and reconfiguration*

When the isolation valves of block 1 are kept open and that of block 2 are closed, if the RCS is found faulty, then block 1 is faulty since the thrusters of block 2 cannot generate any thrust/torque when its isolation valves are closed. Hence, the isolation valves of block 1 are closed and an isolation valve of block 2 is opened, thereby enabling the working of thrusters of block 2. Similar operations are carried out when isolation valves of block 2 are open, while that of block 1 are closed, and the RCS is found faulty.

However, when isolation valves of both the thruster blocks 1 and 2 are open, it is not possible straightaway to identify the faulty thruster block and, therefore, a 'trial-and-error' method is adopted. After failure detection, isolation valves of block 1 are closed, while that of block 2 remain open. If block 1 was faulty, there would not be any further increase in attitude rate and error, since the faulty thruster block 1 is disabled. On the other hand, if thruster block 2 is faulty, attitude error and/or wheel speed will further increase indicating that the fault still exists and the thruster block 2 is faulty. Then, the isolation valves of block 2 are closed and that of block 1 are opened, thereby enabling working of the failure-free thruster block and disabling the faulty one.

Since momentum/reaction wheels and normal mode controllers might not be able to correct fairly large attitude errors and/or rates caused by faulty thrusters, attitude is controlled using thrusters for some time immediately after the autonomous reconfiguration of thrusters, then the normal mode is revived.

8. Simulation results

The proposed fault-tolerance schemes were validated through computer simulations. Attitude dynamics, sensors, controllers, reaction/momentum wheels and

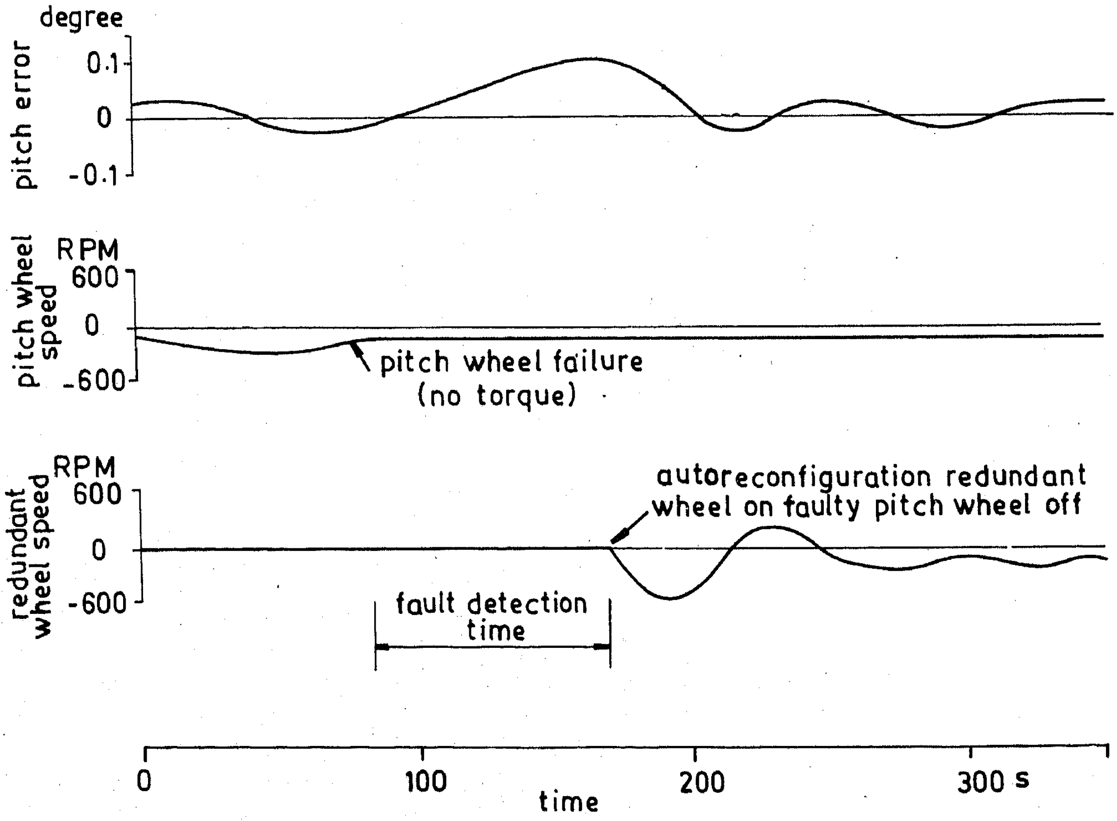


Figure 11. Autoreconfiguration of the pitch wheel.

Table 2. Maximum attitude error before reconfiguration due to stuck-up failure in earth sensor ES.

ESA stuck-up value (degree)	Θ_{max} (degree)	Detection time (S)
0·0	0·50	20·0
0·1	0·40	35·0
0·2	0·30	37·5
0·3	0·15	7·5
0·5	0·15	7·5

NOTE: (i) Θ_{max} is the absolute maximum attitude error before reconfiguration;
(ii) attitude error and rate when fault occurred were 0·1° and 0·01°/s, respectively.

reaction control system were modelled on a digital computer, with provision to simulate different modes of failure of various subsystems. Performance of the fault-detection, identification and reconfiguration (FDIR) algorithms and fault-tolerant system were studied under different failure modes and the performance is satisfactory. Some typical results are given in table 2 and figure 11.

9. Conclusions

With a discussion on the impact of failure of the attitude control system on services rendered by a spacecraft and on mission life, limitations of the existing systems that have redundancy, but need ground-station support for analyses of failures and subsequent remedial actions, are highlighted. The need for autonomous spacecraft attitude control system is emphasized and its essential features are formulated.

Limitations of commonly used schemes for fault tolerance in computers for a real-time control system that consists of dual-redundant attitude sensors and actuators are presented. Though some isolated attempts, like schemes for fault tolerance in attitude reference system using gyros and some theoretical studies on fault detection in a system, were made, there was no comprehensive study to make the entire attitude control system fault-tolerant as yet. A comprehensive study on 'autonomous spacecraft attitude control system through reconfiguration', covering various aspects of the system, is made.

Newly developed autonomous FDIR schemes for dual-redundant earth sensors, attitude reference systems using gyros, reaction/momentum wheel systems and reaction control systems are presented. Also proposed is a new symmetrically-skewed configuration for an attitude reference system using three dynamically tuned-gyros; it has better features than the other configurations.

The proposed schemes are general (or universal) in nature and could be applied to any spacecraft; further, they are relatively simple and hence, do not increase the hardware and software overhead on control electronics much. Also, they do not call for any modification in the already existing and space-proven sensors and actuators. Some of the schemes have already been used in Indian spacecraft. These schemes could be adopted for other applications also with minor modifications.

9.1 *Further challenges*

Though this study covers all major failures in the various elements of attitude control systems that are very critical to a mission, aspects like excessive bias and scale factor errors, and ripple/noise reaction torque from reaction/momentum wheels are not studied in detail; they could be taken up for detailed study. Also, the proposed scheme could be further studied with reference to a specific mission for further refinement and extensive simulations could be carried out.

In addition, the concept of artificial intelligence (AI) and 'learning/expert systems' could be exploited for autonomous on-board evaluation of system performance, decision-making and failure management. Systems that use AI concepts can observe and understand the 'behaviour' of the system, draw 'reasoned conclusions' from the observations and take appropriate decisions like human experts.

As future space missions will directly cater to various applications on an operational basis, the ultimate objective is to have a totally fault-tolerant 'intelligent' autonomous spacecraft.

The authors thank Professor U R Rao, Shri N Pant, Dr K Kasturirangan, and Professor E V Krishnamurthy for motivating them, and for suggestions and guidance. They are also grateful to Professor N Viswanadham, Indian Institute of Science, for inviting them to contribute this paper and for his suggestions. The authors also acknowledge the assistance and cooperation of their colleagues in the Control Systems Division.

List of symbols

D_1, D_2, D_3	dynamically tuned gyros:
e_d	threshold for error difference;
e_u	upper limit for absolute error;
F_i	Boolean variable;
f_{th}	failure threshold;
G	gain factor, Nm/s;
I	moment of inertia of wheel;
L_i	Boolean variable;
P	pitch axis;
P_i	parity equation residual;
R	roll axis;
S	wheel speed, rad/s;
T_r	reaction torque;
T_s	torque control signal;
X_1, X_2, X_3	orthogonal reference axes;
x_1, x_2, x_3,	attitude along three reference axes;
$\hat{x}_1$, $\hat{x}_2$, $\hat{x}_3$	estimates of attitude along X_1, X_2 and X_3, respectively;
Y_{ij}	measurement axis of a DTG;

y_{ij}	output of a DTG;
S_a	actual change in wheel speed;
S_e	expected change in wheel speed;
ξ	measurement noise;
Φ	roll error;
θ	pitch error;
ψ	yaw error;
$\lceil x \rceil$	smallest integer not less than x.

References

Anderson T, Lee P A 1981 *Fault-tolerance: principle and practice* (Englewood Cliffs, NJ: Prentice Hall)

Ammons E E 1979 AIAA paper no. 79 – 17771

Avizienis A 1976 *IEEE Trans. Comput.* C-28: 1304–1312

Bennets R G 1978 *Electron. Power* 24: 845––851

Bennets R G 1979 *Electron. Power* 25: 51–56

Brown R B 1975 *J. Dynamics Syst., Measurement Control* 41–45

Clark R N 1975 *IEEE Trans. Aerosp. Electron. Syst.* AES-11: 465–473

Chen T T, Adams M B 1976 *IEEE Trans Autom. Control* AC-21: 750–757

Daly R C, Gai E, Harrison J V 1979 *J. Guidance Control* 2: 9–17

Engelder P D 1980 *Proc. IEEE Natl. Aerosp. Conf.* (New York: IEEE Press) pp. 330–337

Harrison T, Chen T T 1975 *IEEE Trans. Aerosp. Electron. Syst.* AES-11: 349–357

Harrison J V, Gai E 1977 *IEEE Trans. Aerosp. Electron. Syst.* AES-13: 631–643

Hecht A 1979 *IEEE Trans. Reliab.* R-28: 227–232

Iserman R 1981 *Automatica* 4(6): 17: 387–404

Johnson B W 1984 *IEEE Micro* 4(6): 6–21

Lala P K 1985 *Fault-tolerant and fault testable hardware design* (London: Prentice Hall)

Marie J L 1982 IFAC Conf. automatic control in space, pp. 575–582

McConnel Siewiorek, S R D P 1981 *IEEE Trans. Comput.* C-30: 161–164

Murugesan S 1981 Proc. AIAA Computers in aerospace conference, AIAA paper No. 81–2171, AIAA, San Diego, CA.

Murugesan S 1984a Simulation results on autonomous reconfiguration of reaction wheel system, ISAC/ISRO, Bangalore

Murugesan S 1984b IEEE Int. Conf. Computers, Systems and Signal Processing, 2: 712–716

Murugesan S 1985 *Autonomous fault-tolerant spacecraft control system through reconfiguration*, Ph.D thesis, Indian Institute of Science, Bangalore

Rennels D A 1978 *Proc. IEEE* 60: 1255–1286

Siewiorek D P, Swaz R S 1981 *Theory and practice of reliable system design* (Mass: Digital Press)

Thomson W H 1963 *Introduction to space dynamics* (New York: John Wiley)

Wertz J R 1978 *Spacecraft attitude determination and control* (Dordrecht: Reidel)

Wilsky A S 1976 *Automatica* 12: 601–611

Wilsky A S 1980 *IEEE Trans. Autom. Control* AC-21: 347–360