FAULT-TOLERANT CONTROL - A CASE STUDY OF THE ØRSTED SATELLITE

Søren Abildsten Bøgh and Mogens Blanke [1]

ABSTRACT

The increasing operational requirements for onboard autonomy in satellite control systems necessitates structural methods that support the design of a complete and reliable supervisory system. This paper presents the design strategy used to develop a supervisor for the attitude control system for the Danish Ørsted satellite. The main topic is handling of faults arising in onboard instrumentation, ie. how to detect faults and how to prevent propagation into failures with potential mission loss as a consequence. Formal methods are used to ensure complete coverage of all potential fault types and to guarantee that the design criteria are met in the final implementation.

Keywords: Autonomous Control Systems, Supervisory Control, Fault Detection, Fault Accommodation, Failure Mode and Effect Analysis.

1. INTRODUCTION

The Ørsted Satellite is a micro satellite (approx. 60 kg) with a scheduled launch from Vandenberg, California in spring 1997. The satellite development is made on a low level budget. The level of quality assurance is low and multiple redundant sensors and actuators are avoided. While parallel redundancy systems are required for failsafe systems, this has not been an option here, due to cost and weight. A fault tolerant approach is needed instead to accommodate faults where this is possible and provide graceful degradation when faults occur.

An inevitable consequence of sparse instrumentation is an increased risk for degradation in control capabilities, which must be taken into consideration. The occurrence of faults can be tolerated but it should be prevented that they develop into failures at a subsystem or plant level. Furthermore, it should be guaranteed that all essential faults are detected and all critical faults are accommodated. Manual interaction from ground is inadequate for the Ørsted satellite, as the operation is controlled from only one ground station, situated in Denmark. This means that there will be only 2-3 contact periods of 10 minutes each day. Therefore, autonomous operation and on-board fault handling is required to avoid serious impact on the scientific mission or even loss of the satellite. Some of the functionality that is traditionally implemented on ground stations must, consequently, be moved to the space segment.

This work addresses the problem of design of an autonomous supervisor for attitude control. A method is suggested that gives a consistent design and assures system dependability. The basic philosophy is to use all existing sensors and actuators to make systematic use of both direct and indirect redundancy in the available information. Generally, fault handling is a three step procedure, where the first step is detection of a non-normal condition. The second step is to isolate the cause to one or more possible component faults. The third step is to evaluate the condition, take decision about activation of actions to accommodate the fault and finally enforce the remedy action.

[1] Department of Control Engineering, Aalborg University
Fredrik Bajers Vej 7, DK 9220 Aalborg Ø, Denmark

There has been a wide interest in the field of fault detection and isolation algorithms (FDI) (Refs. 24-35), and some attention to fault accommodation (Refs. 16-23), but almost no work in the field of general fault handling and how to obtain a complete and consistent supervisor logic. An overall approach was taken in ref. 2, where abnormal controller operation and tuning are key issues. A general FDIA system was treated by ref. 3 for a narrow scenario where state feedback was required and faults needed to be state disturbance signals, similar to actuator faults.

This paper contributes with a new approach to examine faults in control systems and with development of a supervisory level in a systematic and consistent manner. A general design strategy is proposed that incorporates existing software tools in the development of an integrated system with both fault detection and accommodation.

The proposed design strategy is illustrated by application to the Attitude Control System (ACS) of the Danish Ørsted satellite. The concept is, however, suitable to principally any attitude control system.

2. THE ØRSTED SATELLITE

The main purpose of the Ørsted satellite is to collect measurements of the geomagnetic field and high energy particle activity in a near-Earth orbit. The main body carries antennas, solar panels, electronic equipment and an 8 meter boom.

After ejection from the launch vehicle into an elliptical, low altitude, polar orbit the satellite is captured from a random tumbling (this is called the tumbling phase). Once the satellite is stabilized and ground contact is established the boom is deployed. The remaining part of the mission is called the operational phase and the task of the Attitude Control System (ACS) is to point the boom away from the Earth.

Attitude is measured with a star camera or alternatively with a three axis magnetometer and sun sensors. Active attitude control is achieved by magnetic torquing using a 2-redundant, three axis magnetorquer configuration. It is possible that sensor signals are invalid or are missing because faults can occur in any instrument. Furthermore, the availability of a star camera output is limited as it gives no output when the Earth or the Sun is inside it’s field of view.

The fundamental requirement to dependability of the ACS is that no single point failure shall cause loss of the spacecraft. If something goes wrong, the most important thing is to know what went wrong. This means that the communication link is essential. Ground communication is only possible if the satellite motion is reasonable small and there is sufficient power on the batteries. This boils down to three basic requirements that, in case of single point failures, the ACS system shall

- avoid excessive spin-up of the satellite, and
- avoid large power consumption for long periods, and
- maintain three axis attitude stabilization if this is at all possible.

In this paper the faults associated with the electronics driving the magnetorquers are selected to illustrate the fault handling concept, as a complete description of all instrument faults would be too extensive. The six magnetorquers are arranged in two sets, A and B, each with one magnetorquer in x-, y-, and z-directions. Two magnetorquers on the same axis are used with the principle that the A-coil is the primary and if saturated, the B-coil is activated to carry the remaining current.

A principal diagram of the coil driver electronics and a magnetorquer is shown in Figure 1. The coil current is controlled by a regulator where the actual current is measured by a shunt resistor. The current request is delivered on a dedicated line, called Paste Bus. The current direction (sign) is controlled by dedicated switching logic. The current is measured as the voltage above the shunt resistor and indicates the unsigned current amplitude.

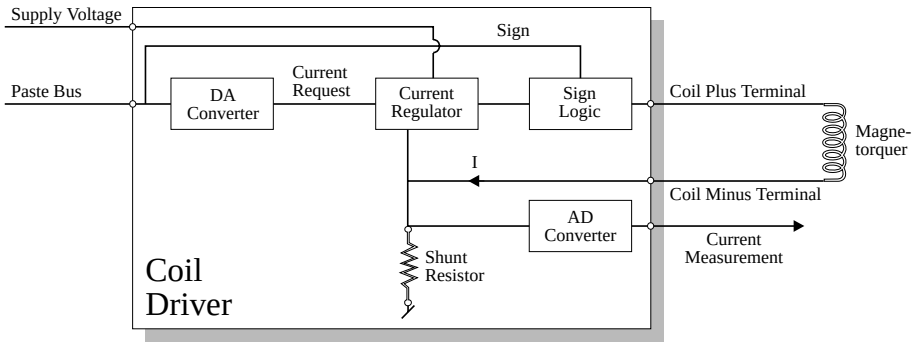

Figure 1 *: Principal diagram of a single coil driver and magnetorquer. Desired currents are requested through the Paste bus and a current regulator controls the current. A measurement of the absolute value of the current is available.*

3. SUPERVISOR DESIGN METHODOLOGY

It is important that the complete design of the integrated supervised control system follows a modular approach, where each functionality can be designed, implemented, and tested independently of the remaining system. The algorithms that realise the supervisory functionality constitute themselves an increased risk for failures (in the software), so the overall reliability can only be improved if the supervisory level is absolutely trustworthy.

Earlier work on fault modelling, fault analysis and the special problem of faults in feedback loops is available in ref. 4, 5, 6, and 7.

This chapter introduces a seven-step design procedure that leads to an improved supervisor compared to what is obtainable by conventional ad-hoc methods. The design procedure is dedicated to a unique implementational architecture, which has proven to be suitable for real-time realisations. The architecture is first described.

3.1. Architecture

The implementation of an additional supervisory level onto a control system is not a trivial task. The architecture shall accommodate the implementation of diverse functions, where, for the Ørsted satellite, the following list comprise the operational requirements:

- Mission phase control (tumbling phase, operational phase).
- Operational mode control (different attitude determination methods are used if the star camera data is available or not).
- Onboard monitoring (of operational status, control error, eclipse conditions).
- Fault handling.
- Command and telemetry interface.

These functions are adequately implemented in a supervisory structure with three levels as shown in Figure 2:

1. A lower level with input/output and the control loop.
2. A second level with algorithms for fault detection and fault accommodation.
3. A third level with supervisor logic.

The Control Level is designed and tested in each individual mode that is specified by different operational phases and different instrumentation configurations. The miscellaneous controller modes are considered separately and it is left to the supervisor design to guarantee selection of the correct mode in different situations.

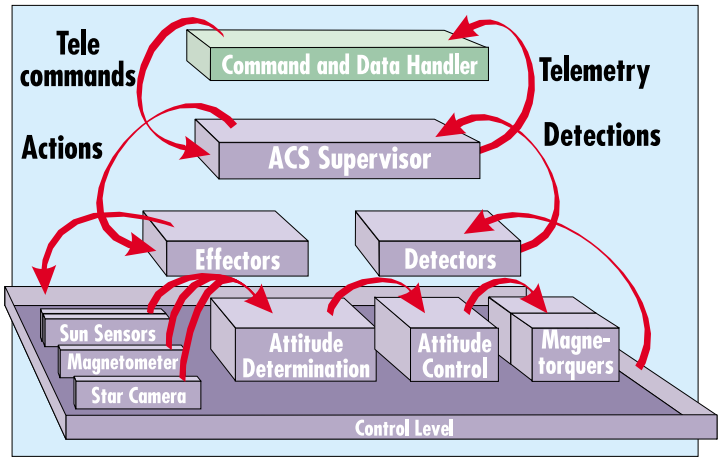

Figure 2 *: Structure of ACS with supervisor for fault handling and telecommand/telemetry interface.*

The Detectors are signal processing units that observe the system and compares with the expected system behaviour. An alarm is raised when an anomaly is detected. The Effectors execute the remedy actions associated with fault accommodation.

The Supervisor reacts on the current condition, receiving inputs from detectors and commands from the satellite command distributor. From a set of logical rules, the supervisor determines the appropriate actions to be executed on the control level and the telemetry to be generated.

3.2. Design Strategy

When the level of onboard autonomy becomes extensive and thereby demands a higher level of reliable operation, it becomes inherently more complex for the designer to cover all possible situations and guarantee correct and complete operation. It is therefore important to use a systematic design strategy that first of all promotes a complete examination of all possible faults and also favours easy iteration between individual design steps.

This chapter describes the design procedure which involves a broad range of aspects. It is crucial, that the supervisor implementation agrees with the design requirements, and a method to support this is introduced.

The rules of the supervisor are designed and checked using the design procedure shown in Figure 3. A short summary of the design steps follows below, and a detailed description can be found in ref 5.

1) A Failure Mode and Effects Analysis (FMEA) of all involved sub-systems (magnetorquer power drives, star camera, sun sensors, CSC magnetometer, etc.) is performed and combined into a complete analysis of the entire satellite. The end-effects describe consequences on top level (eg. satellite tumbling, control error increases, etc.). The FMEA technique used in this context is described in ref 4.

2) The top level end-effects are judged for severity, and the ones with significant influence on the control performance are selected to be handled by the supervisor.

3) The possibilities of fault accommodation are considered. This includes enabling and disabling of redundant units (magnetorquers, power drives, and sun sensors), selection between the two attitude estimation algorithms (normal and secondary operational mode), and otherwise graceful degradation and close down. The point of reconfiguration determines the requirements for fault isolation. It is not necessary to isolate faults below the level where the fault effect propagation can be stopped.

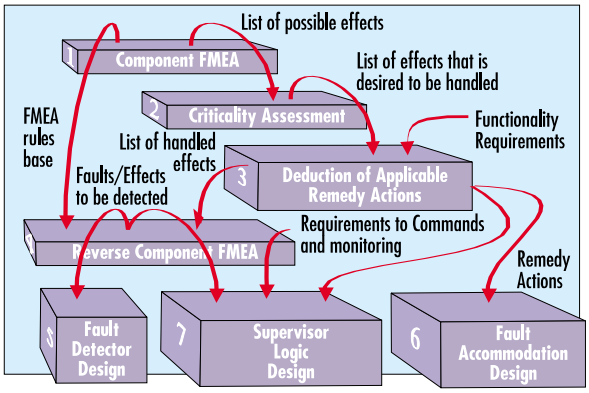

Figure 3. *Systematic supervisor design approach. These seven actions conduct the designer from an analysis of failures to the design of fault detectors, supervisor logic, and fault accommodation.*

4) A reverse deduction of the FMEA rule base is performed to locate the faults that cause the considered end-effects. The deduction is performed down to the point of reconfiguration as determined in step 3.

5) Fault detector algorithms are designed. Most fault events are detected by simple means like range and rate check on sensor signals, but also the magnetic coupling from the magnetorquers to the magnetometer is exploited to catch anomalies in the power drives and magnetorquers. Isolation of sun sensor faults uses innovations from an extended Kalman filter used in the alternative attitude acquisition.

6) Fault accommodation actions are designed. The Ørsted supervisor involves only simple selection of control level algorithms, enabling and disabling of redundant hardware, and activation/deactivation of the entire controller.

7) Supervisor inference rules are designed using the information about which faults/effects are detected and how they are accommodated. The supervisor determines the most appropriate action from the present condition and commands. Supervisor realization using extended state-event machines and object oriented approaches in a meta-class architecture are introduced in ref 7.

These steps are followed to make the supervisor design cheaper, faster, and better. The fault coverage is then (hopefully) as complete as possible, because the FMEA step includes in principle all possible faults. The analysis is modular, because small sub-systems are treated individually. Furthermore, the strategy has the advantage that the system is analyzed on a *logical* level as far as possible before the laborious job of mathematical modelling and design is initiated. This ensures that superfluous analysis and design are avoided.

4. ØRSTED SATELLITE ATTITUDE CONTROL

To illustrate the design strategy introduced in the previous chapter, some examples from the Ørsted satellite's attitude control system design are presented. The failure analysis and fault detection are illustrated by an actuator fault while the supervisor inference rule design is illustrated by a sensor fault.

4.1. Component FMEA

Following the procedure given in chapter 3, the first step in the design procedure is to carry out a Failure Mode and Effect analysis for the relevant components. The level of detail in the analysis is chosen by the designer, depending on the knowledge he has about the system. In this case, each coil driver and the corresponding magnetorquer are considered as one unit. The remaining elements are the satellite dynamics model, all attitude sensors, and the attitude controller. From the controller, the failure propagation path loops back to the coil drivers. Since the focus of this paper is on faults in the coil drivers, it is not interesting to

know the details of the failure propagation through the satellite motion to the sensors and finally the controller, and the analysis is also rather complex. The important question is how the coil driver faults influence the control performance. These end-effects can be determined by simulation, so the satellite dynamics, the sensors, and the control algorithm are considered as one unit in this FMEA and placed on the second level of analysis.

All potential faults for each of the six coil drivers and coils are shown in Table I. Faults are named with F_{ijk} and effects with E_{ijk}, where i is the fault/effect index, j is the unit index and k is the level.

Effect / Item	E_{111}: Low magnetic moment *(m = 0)*.	E_{211}: Maximum magnetic moment *($m=nAI_{max}$)*	E_{311}: Magnetic moment has negative sign.	E_{411}: Magnetic moment has positive sign.	E_{511}: Magnetic moment unchanged *m(t) = m(t-1)*
Input	F_{111}: Supply voltage Low.				F_{211}: Paste Bus command error
Part	F_{311}: Coil wire disconnected F_{411}: Shunt resistor disconnected F_{511}: Coil connector plus terminal short circuit to ground or to Coil connector minus terminal.	F_{611}: Shunt resistor short circuit F_{711}: Coil connector minus terminal short circuit to ground.	F_{811}: Sign bit failed negative.	F_{911}: Sign bit failed positive.	

Table I : *FMEA of one of the six units consisting of coil driver and coil. F_{ijk} indicates fault and E_{ijk} indicates effect.*

The effects from the six coil driver units on the first level of analysis are propagated to the second level with the satellite and control unit as seen in Figure 4.

The end-effects shown in Figure 4 are simulated and have the following interpretations:

E_{112}: Detumbling failed, random tumbling continues.
E_{212}: Capture time increased, steady state control error increased significantly.
E_{312}: Power consumption increased.
E_{412}: Capture time increased slightly, small increment in steady state control errors.
E_{512}: No effect.

4.2. Severity Assessment

The end-effects listed above are assigned a severity level and grouped into two classes: The effects that shall be handled, and the effects that can be handled (Table II).

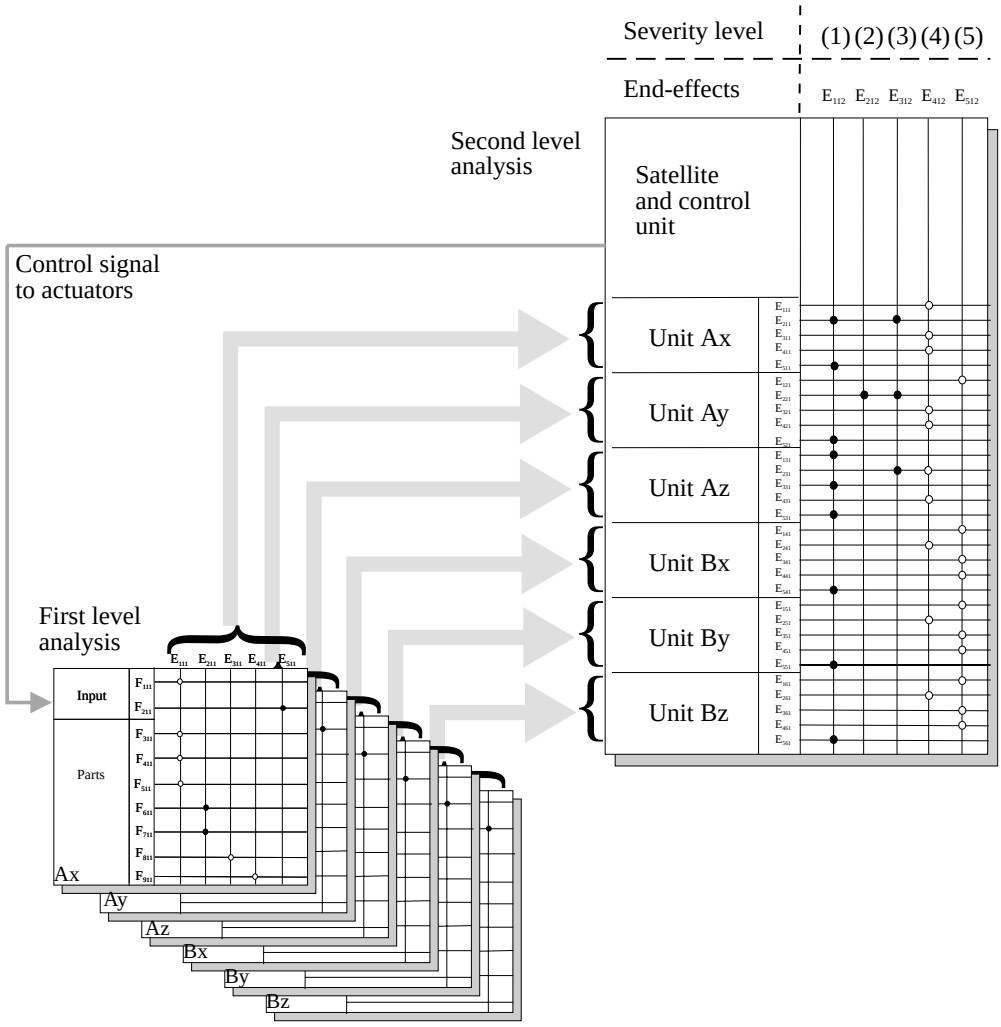

Figure 4 *: Graphical illustration of the complete FMEA analysis of potential faults in the Ørsted satellite actuators.*

Effects on Satellite Control		Severity Level		Fault Handling
E_{112} E_{212} E_{312}	Detumbling failed, random tumbling continues Capture time and control error increased significantly. Power consumption increased.	1 2 3	Catastrophic Very serious Serious	*Shall* be handled
E_{412} E_{512}	Capture time and control error increased slightly. No effect.	4 5	Not serious Indifferent	*Can* be handled

Table II *: Fault effects on the satellite and corresponding severity levels.*

The first class indicates faults that have a critical consequence on the satellite mission and the other class indicates faults with no significant effect on the satellite mission. It is thus not a requirement that faults in the second class shall be detected.

An interesting observation in the FMEA is that the same type of fault in different magnetorquers have different effects. For instance, it can be seen in Figure 4 that if the shunt resistor in coil driver Ax short circuits (F_{611}), the catastrophic consequence is random tumbling and increased power consumption (E_{112} and E_{312}). The same fault in unit Bx (F_{641}) only causes slightly decreased control performance (E_{412}) which is not serious.

4.3. Deduction of Applicable Remedy Actions and Fault Accommodation Design

The possible remedy actions on the Ørsted satellite are very limited because the instrumentation is simple and the on-board computing facilities are restricted. The following remedy actions are possible:

1 If a magnetorquer in set A, ie. Ai ($i \in \{x, y, z\}$), is detected faulty, then use the corresponding magnetorquer in set B.
2 In more severe cases, where full three axis control is not possible, the control system shall be closed down.

None of these remedy actions employ advanced modifications of the control level and can be achieved by simple fault accommodation.

4.4. Reverse Component FMEA

The next step is to locate all faults that caused the effects, which shall be handled. This is done by abduction through the component FMEA rule base obtained in step 1. The abduction is rather simple and shows up to give the following list of faults that must be detected:

- Paste Bus send command status (send successful or failed).
- Range check on measured current.
- Difference between desired current and measured current.
- Discrepancy between generated magnetic moment and magnetic field measurement.

4.5. Fault Detector Design

The fault detectors shall detect the effects listed above. In the sequel the different methods required to complete this obligation are introduced. Only simple methods are used, because the requirement to software size is very strict. Analytical redundancy methods, that utilize the non-linear dynamics of the satellite, are thus not applicable.

Paste Bus Error Detection

The effects $\{E_{511}, E_{521}, E_{531}, E_{541}, E_{551}, E_{561}\}$ are caused by an error on the Paste Bus. When a coil current request or a current measurement request is transferred to the coil driver, the status of the Paste Bus is returned from the low level driver. If the send operation failed, the corresponding coil driver is declared faulty.

Range check on current measurement

The effects $\{E_{211}, E_{221}, E_{231}\}$ correspond to currents which are outside the legal operating range. This can be determined by range check on the current measurement. If a current is outside the range [-0.55, 0.55] ampere, the corresponding coil driver is declared faulty.

Test difference between desired current and current measurement.

The effect $\{E_{131}\}$ is caused by zero current in the coil Az. This type of fault is present if the numerical difference between the desired current output and the measured current is significant and the measured current is close to zero.

It has been assumed, so far, that the current measurement could not be erroneous. There is, of course, a certain likelihood for a measurement fault to raise an alarm, albeit there is no influence on the satellite. This is accepted because the measurement is vital to confirm the actual current.

Discrepancy between generated magnetic moment and magnetic field measurement.

The effect $\{E_{331}\}$ is caused by a fault in the Az coil driver sign logic, so the actual current is always negative, even when positive currents are desired. This fault cannot be detected from the current measurement, as this indicates the unsigned value.

This problem is solved by using the magnetic field measurement. When the boom is stowed, the magnetorquer currents disturb the magnetic field measurement. This can be used to confirm that the currents requested to the coils are actually in effect. The disturbance is computed by multiplying a 3x3 transformation matrix $\boldsymbol{A}$ to the sum of the currents in the same axis:

$$\boldsymbol{B}_{Magn} = \boldsymbol{A}\ (\boldsymbol{I}_A + \boldsymbol{I}_B) \tag{1}$$

A residual can thus be computed as the difference between the desired currents and the estimation of the actual currents:

$$\boldsymbol{r} = (\boldsymbol{I}_{Desired,A} + \boldsymbol{I}_{Desired,B}) - \boldsymbol{A}^{-1}(\boldsymbol{B}_{Total} - \boldsymbol{B}_{Geo}) \tag{2}$$

$\boldsymbol{B}_{Total}$ is a measurement when the coils are active and $\boldsymbol{B}_{Geo}$ is a measurement when the coils are not active. There is a time difference between the two measurements which causes a deviation in the expected geomagnetic field caused by the rotation of the satellite. This causes the residual to be large when the angular velocity is large. The problem is solved by increasing the testing threshold when the angular velocity is large. The angular velocity is estimated from the rate of change of the geomagnetic field measurement. The increased threshold leads, of course, to the inevitable problem that the sensitivity to faults during periods with large angular velocity decrease. The details of these calculations are left out of this paper.

Another problem is the isolation between faults in coil driver set A and B. The two currents in eq.(1) act additive and cannot be separated completely. But, as only sign failures are considered, it is possible to distinguish the faults when the two requested currents are significantly different.

4.6. Supervisor Logic Design

The attitude control system for a small satellite like Ørsted would immediately seem rather uncomplicated, but there may be interconnections between sub-systems which in the run-time system cause the supervisor to deviate from the design aims. An obvious innocent cross correlation may be neglected and show up to be significant. This section illustrates how a computer toolbox for boolean logic processing is used to prove correctness. The presentation uses, as an example, the second case study - a star camera failure, which is a sensor malfunction.

The supervisor rules designed in step 7 (see above) are implemented in the Beologic Array Inference Toolbox (AIT) (ref 15). This is a commercial product from Bang & Olufsen (Denmark) that supports the analysis of logical networks. AIT is used during the design phase to make a completeness check of the supervisor logic for fault handling to verify that the fault accommodation actually stops the propagation of faults, and that it is consistent with the design requirements. This is done by implementing rules for the complete logical data flow of the reconfigurable system as illustrated in Figure 5.

The figure shows the logical data flow of fault propagation (true or false) from sub system FMEA to top level consequences as end-effects. The rules of the fault detectors simply states (true or false) that a certain fault effect can be detected or not. The supervisor represents the exact run-time rules that use the boolean fault detections to determine remedy actions. These actions are now written in AIT as rules that disable the propagation of faults, as it would do in the real implementation. In a logical sense, the termination of fault propagation means that the fault effect is no longer active and hence the corresponding detection will be false. This fact constrains the faults that are successfully accommodated to be forced in-active. If they were true there would be a contradiction in the rule base. A very powerful completeness check of the supervisor rules is based on this *logical feedback*. The rule base is automatically checked and a list of faults bound to false is generated. The list is examined to verify that all the faults expected to be accommodated actually are handled by the

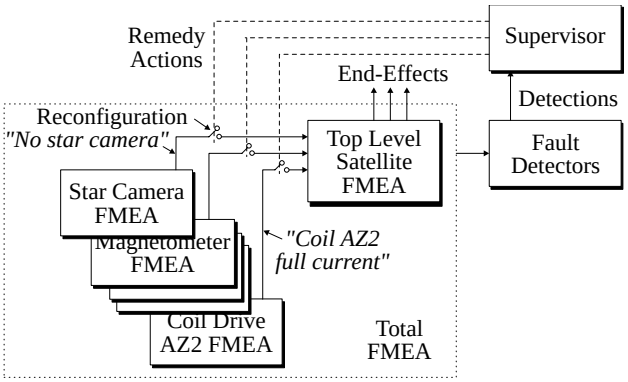

Figure 5. *The principle of fault detection and reconfiguration. A fault that occurs in some sub-system will propagate through the system, be identified by a detector, and the supervisor reconfiguration will stop the fault propagation.*

supervisor rules.

A simple example on the check for supervisor rule base completeness is the star camera (SIM) black out handling. The propagation of a black out (`SIMFault=true`) is given by the rule:

```
SIMFault_ = (AD_OP_NO and SIMFault)
```

which states that the SIM fault will have the effect `SIMFault_=true` when the SIM is used for attitude determination (`AD_OP_NO=true`). The SIM fault will propagate through the top level FMEA and cause the satellite to experience a random tumbling motion:

```
RandomMotion =    ((Phase_Normal and (ADUncertHigh_ or SSA1Low_ or SSB1Low_ or SIMFault_))
                   or CSCFault_ or CD2MMax_ or CD3MPos_)
```

In this rule, numerous other causes for the same end-effect are included, but these are not essential in this context. It should be noticed, anyhow, that the SIM fault only causes an effect when the satellite is in the science observation phase, where the boom is deployed (`Phase_Normal=true`). A SIM fault is easily detected because the star camera will stop the generation of data. Hence, the detector rule simply states that a SIM fault is detected:

```
DET_Sim_Fault = SIMFault_
```

When a SIM fault is detected the supervisor will disable SIM based attitude estimation (`AD_OP_NO=true`) and switch to the alternative algorithm using sun sensors and magnetometer instead (`AD_OP_NO=false`):

```
(Phase_Normal and !DET_Sim_Fault) = AD_OP_NO
```

It is easy for this small rule base to see that the variable `SIMFault_` *cannot* be true and correct supervisor reconfiguration is thus confirmed. The entire Ørsted supervisor rule base is much more complicated so it is advantageous to use a computer tool to support this verification.

5. RESULTS

The attitude control system supervisor is implemented on the Ørsted satellite in a multitasking ADA software environment. The layered architecture from Figure 2 is implemented using two separate tasks -one for the control level and one for the supervisor. This is advantageous for detailed design and test, but also during run-time because the two loops are not required to execute with the same sampling time. The non-synchronous execution does introduce some problems with the availability of information, but these can be solved.

A complete test of the augmented attitude control system is far too voluminous for this presentation, so only

two examples are given, one for a an actuator failure and one for a sensor failure.

5.1. Actuator Failure

A simulation of detumbling control with a short circuit in the Ax coil driver is shown in Figure 6. The graphs depict the attitude control performance with and without a fault in the coil driver. During the tumbling phase the angle between the satellite *z*-axis and the local geomagnetic field vector **B** is preferably 180˚, but in case of a coil driver malfunction, it increases significantly as seen in the figure. If the defect coil driver is replaced by the redundant Coil Bx, the controller performance can be maintained without degradation. This example clearly illustrates the necessity of fault handling.

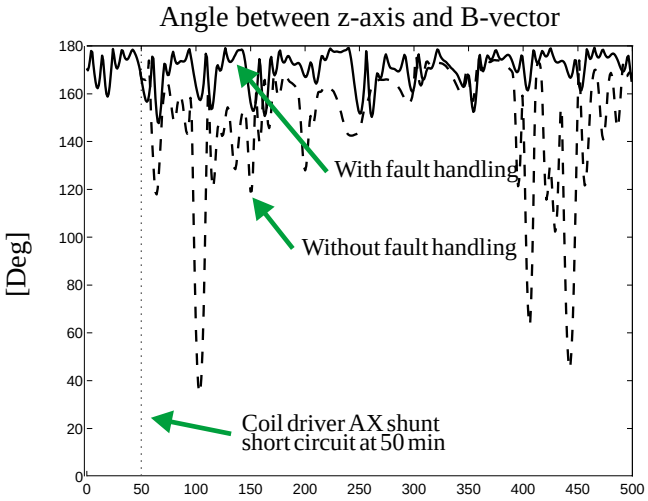

Figure 6 *: Illustration of the consequence on satellite attitude if a coil driver fault is not handled. The control error is normally within 30˚, but if the fault is not accommodated, the error increases up to 150˚.*

5.2. Sensor Failure

An example on a sensor failure is a black out of the primary attitude acquisition sensor, the star camera. Combined attitude control and estimation results are shown in Figure 7 for a situation with star camera blackout. The attitude errors are referred to the nominal attitude.

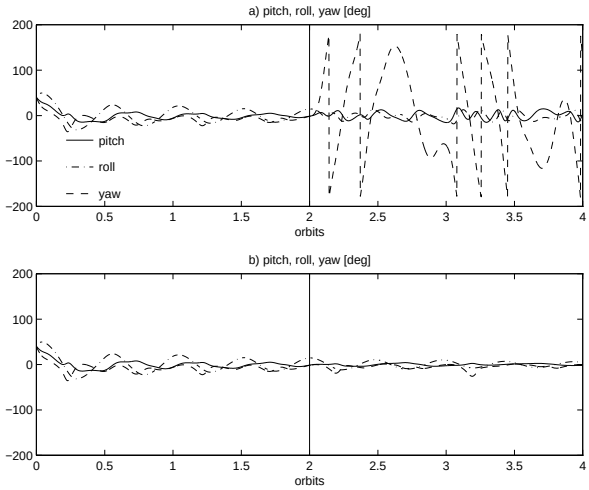

Figure 7*. Simulated attitude determination and control. Star camera blackout after 2 orbits. In plot a) no reconfiguration is performed. In b) the attitude determination is reconfigured.*

The initial attitude is 40˚ in all three angles and the star camera is simulated to black out after two orbits. The two simulations clearly show the necessity to reconfigure attitude acquisition to be based on sun sensors and magnetometer instead of the star camera. If no reconfiguration takes place, the satellite will begin rotating about the boom axis.

6. CONCLUSION

This paper presented a formal strategy for the design of dependable control systems, where explicit knowledge about faults in instrumentation is used to prevent faults from propagating into serious or catastrophic failures. It was shown, how important it is to use a methodical approach to develop a complete catalogue of faults and their consequences. The particular method, FMEA (Failure Mode and Effect Analysis), was selected as an appropriate technique that could be automated. The knowledge about faults and their effects were used to identify the precise remedy action that terminates the fault propagation. The information about faults and remedy actions were compiled together with other requirements (operator interface commands and monitoring generation) in the constraint solving toolbox Beologic. It was shown, that easy iterations during design and implementation could be improved by automated reasoning.

The strategy presented was applied to the design of the attitude control system of the Danish Ørsted satellite. This illustrated the potential of using systematic design methods to achieve increased reliability of control systems for small mission satellites. It was demonstrated, how important it is to consider fault handling in an early design step, as this gives a suitable structure of the complete supervised control system. This paper proposed a layered structure that not only promotes modular design, but also gives a software structure that makes implementation and test easy and very suitable for object oriented programming languages.

7. REFERENCES

1 Warwick, K, Tham, M T 1991, *Failsafe Control Systems. Applications and Emergency Management*, Chapmann and Hall, London, ISBN 0 412 37740 3.

2 Åström, K J, Anton K E 1986, Expert Control, *Automatica*, Vol. 22, pp.227-286.

3 Tsui, C A 1994, A general failure detection, isolation and accommodation system with model uncertainty and measurement noise, *IEEE Transactions on AC*, Vol. 39, No. 11, Nov. 1994, pp.2318-2321.

4 Blanke, M, Jørgensen, R B, Svavarsson, M 1995, A New Approach to Design of Dependable Control Systems, *Proc. 40. KoREMA*, Zagreb, Croatia, April 1995.

5 Bøgh, S A, Zamanabadi, R I, Blanke, M 1995, Onboard Supervisor for the Ørsted Satellite Attitude Control System, *ESA/ESTEC Workshop "AI and KBS for Space"*, Oct. 95, Nordwijk, Holland.

6 Blanke, M 1996, Consistent Design of Dependable Control Systems, *Control Engineering Practice*, Vol 4, No 9, pp.1305-12.

7 Blanke, M, Zamanabadi, R I, Bøgh, S A, Lunau, C P 1997, Fault-tolerant Control Systems - a Holistic View, Accepted for publication in *Control Engineering Practice*.

8 Legg, J M 1978, Computerized Approach for Matrix-Form FMEA, *IEEE Trans. on reliability*, Vol R-27, No 1, pp.154-157.

9 Herrin S A 1981, Maintainability Applications Using the Matrix FMEA Technique, *IFAC's Transactions on reliability*, Vol R-30, No 3, pp.212-217.

10 Yuan, J 1985, A Strategy to Establish a Reliability Model with Dependent Components through FMEA, *Reliability Engineering*, Vol 11, pp.37-45.

11 Bell, T E June 1989, Managing Murphy's Law: Engineering a Minimum-Risk System, *IEEE Spectrum*, pp.24-27.

12 Møller, G 1995, *On the Technology of Array-based Logic*. Ph.D. thesis. Electric Power Eng. Dept. Tech. University of Denmark, Lyngby, Denmark.

13 Franksen, O I 1978, Group Representations of Finite Polyvalent Logic - a Case Study Using APL

Notation. *Proc. IFAC World Congress*, Helsinki, pp.875-887.

14 More, T 1981, Notes on the Diagrams, Logic and Operations of Array Theory. In: *Structures and Operations in Engineering Management Systems*, (eds: Ø. Bjørke and O.I.Franksen) Tapir.

15 Bang & Olufsen, 1996, *BEOLOGIC: Array Inference Toolbox, User's Manual, Personal Computers*, Bang & Olufsen, Struer, Denmark.

16 Moerder, D D, Halyo, N, Broussard, J R, Caglayan, A K 1989, Application of Precomputed Control Laws in a Reconfigurable Aircraft Flight Control System, *AIAA J. Guidance*, Vol 12, No 3, pp.325-333.

17 Patton, R J 1991, Fault Detection and Diagnosis in Aerospace Systems using Analytical Redundancy, *IEE Computing & Control Eng. Journal*, Vol 2, No 3, pp.127-136.

18 Eterno, J S, Weiss, J L, Looze, D P, Willsky, A 1985, Design Issues for Fault Tolerant-Restructurable Aircraft Control, *IEEE Proceedings of the 24th Conference on Decision & Control*, Vol 2, pp.900-905.

19 Morse, W D, Ossman, K A 1990, Model Following Reconfigurable Flight Control System for the AFTI/F-16, *AIAA J.Guidance*, Vol 13, No 6, pp.969-976.

20 Huang, C Y, Stengel, R F 1990, Restructurable Control Using Proportional-Integral Implicit Model Following, *AIAA J. Guidance*, Vol 13, No 2, pp.303-309.

21 Gao, Z, Antsaklis, P 1991, Stability of the Pseudo-Inverse Method for Reconfigurable Control Systems, *Int.J.Control*, Vol 53, No 3, 1, pp. 717-29.

22 Ahmed-Zaid, F, Ioannou, P, Gousman, K, Rooney, R 1991, Accommodation of Failures in the F-16 Aircraft Using Adaptive Control, *IEEE American Control Conf.*, pp.73-78.

23 Ochi, Y, Kanai, K 1991, Design of Restructurable Flight Control Systems Using Feedback Linearization, *AIAA J.Guidance* Vol 14, No 5, pp.903-911.

24 Ray, A, Luck R. 1991, An Introduction to Sensor Signal Validation in Redundant Measurement Systems, *IEEE Control Systems*, Vol 11, No 2, pp.44-48.

25 Tzafestas, S, Watanabe, K 1990, Modern Approaches to System/Sensor Fault Detection and Diagnosis, *Journal A.*, Vol 31, No 4, pp.42-57.

26 Gertler, J 1991, Analytical Redundancy Methods in Fault Detection and Isolation, *IFAC Proceedings to SafeProcess '91*, Vol 1, pp.9-21.

27 Patton, R, Frank, P, Clark, R 1989, *Fault Diagnosis in Dynamic Systems. Theory and Application*, Prentice Hall International.

28 Ding, X, Frank, P M 1994, Comparison of Observer-based Fault Detection Approaches, *IFAC Proceedings to SafeProcess '94*, Vol 2, pp.556-561.

29 Isermann, R 1994, Integration of Fault Detection and Diagnosis Methods, *IFAC Proceedings to SafeProcess '94*, Vol 2, pp.597-612.

30 Isermann, R 1984, Process Fault-Detection based on Modelling and Estimation Methods - A Survey, *Automatica*, Vol 20, No 4, pp.387-404.

31 Ding, X, Frank, P M 1991, Frequency Domain Approach and Threshold Selector for Robust Model-based Fault Detection and Isolation, *Proc. IFAC/IMACS Symposium. SafeProcess '91*, Vol 1, pp.307-312.

32 Emani-Naeini, A, Athter, M M, Rock, S M 1988, Effect of Model Uncertainty on Failure Detection: the Threshold Selector. *IEEE AC*, Vol. 33, No. 12, Dec. 1988, pp.1106-1115.

33 Basseville, M, Nikiforov, I V 1993, *Detection of Abrupt Changes: Theory and Application*, Prentice Hall. New Jersey.

34 Watanabe, K, Matsuura, I, Abe, M, Kubota, M, Himmelblau, D M 1989, Incipient Fault Diagnosis of Chemical Processes via Artificial Neural Networks, *AiChE Journal*, Vol 35, No 11, pp.1803-1812.

35 Frank, P M 1994, Application of Fuzzy Logic to Process Supervision and Fault Diagnosis, *IFAC Proceedings to SafeProcess '94*, Vol 2, pp.531-538.