Paris, 19 July 1996

ARIANE 5

Flight 501 Failure

Report by the Inquiry Board

The Chairman of the Board :

Prof. J. L. LIONS

FOREWORD

On 4 June 1996, the maiden flight of the Ariane 5 launcher ended in a failure. Only about 40 seconds after initiation of the flight sequence, at an altitude of about 3700 m, the launcher veered off its flight path, broke up and exploded. Engineers from the Ariane 5 project teams of CNES and Industry immediately started to investigate the failure. Over the following days, the Director General of ESA and the Chairman of CNES set up an independent Inquiry Board and nominated the following members :

- Prof. Jacques-Louis Lions (Chairman) Acad emie des Sciences (France)
- Dr. Lennart L beck (Vice-Chairman) Swedish Space Corporation (Sweden)
- Mr. Jean-Luc Fauquembergue De l egation Ge ne rale pour l'Armement (France)
- Mr. Gilles Kahn Institut National de Recherche en Informatique et en Automatique (INRIA), (France)
- Prof. Dr. Ing. Wolfgang Kubbat Technical University of Darmstadt (Germany)
- Dr. Ing. Stefan Levedag Daimler Benz Aerospace (Germany)
- Dr. Ing. Leonardo Mazzini Alenia Spazio (Italy)
- Mr. Didier Merle Thomson CSF (France)
- Dr. Colin O'Halloran Defence Evaluation and Research Agency (DERA), (U.K.)

The terms of reference assigned to the Board requested it

- to determine the causes of the launch failure,
- to investigate whether the qualification tests and acceptance tests were appropriate in relation to the problem encountered,
- to recommend corrective action to remove the causes of the anomaly and other possible weaknesses of the systems found to be at fault.

The Board started its work on 13 June 1996. It was assisted by a Technical Advisory Committee composed of :

- Dr Mauro Balduccini (BPD)
- Mr Yvan Choquer (Matra Marconi Space)
- Mr Remy Hergott (CNES)
- Mr Bernard Humbert (Aerospatiale)
- Mr Eric Lefort (ESA)

In accordance with its terms of reference, the Board concentrated its investigations on the causes of the failure, the systems supposed to be responsible, any failures of similar nature in similar systems, and events that could be linked to the accident. Consequently, the recommendations made by the Board are limited to the areas examined. The report contains the analysis of the failure, the Board's conclusions and its recommendations for corrective measures, most of which should be undertaken before the next flight of Ariane 5. There is in addition a report for restricted circulation in which the Board's findings are documented in greater technical detail. Although it consulted the telemetry data recorded during the flight, the Board has not undertaken an evaluation of those data. Nor has it made a complete review of the whole launcher and all its systems.

This report is the result of a collective effort by the Commission, assisted by the members of the Technical Advisory Committee.

We have all worked hard to present a very precise explanation of the reasons for the failure and to make a contribution towards the improvement of Ariane 5 software. This improvement is necessary to ensure the success of the programme.

The Board's findings are based on thorough and open presentations from the Ariane 5 project teams, and on documentation which has demonstrated the high quality of the Ariane 5 programme as regards engineering work in general and completeness and traceability of documents.

Chairman of the Board

1. THE FAILURE

1.1 GENERAL DESCRIPTION

On the basis of the documentation made available and the information presented to the Board, the following has been observed:

The weather at the launch site at Kourou on the morning of 4 June 1996 was acceptable for a launch that day, and presented no obstacle to the transfer of the launcher to the launch pad. In particular, there was no risk of lightning since the strength of the electric field measured at the launch site was negligible. The only uncertainty concerned fulfilment of the visibility criteria.

The countdown, which also comprises the filling of the core stage, went smoothly until H0-7 minutes when the launch was put on hold since the visibility criteria were not met at the opening of the launch window (08h35 local time). Visibility conditions improved as forecast and the launch was initiated at H0 = 09h 33mn 59s local time (=12h 33mn 59s UT). Ignition of the Vulcain engine and the two solid boosters was nominal, as was lift-off. The vehicle performed a nominal flight until approximately H0 + 37 seconds. Shortly after that time, it suddenly veered off its flight path, broke up, and exploded. A preliminary investigation of flight data showed:

- nominal behaviour of the launcher up to H0 + 36 seconds;
- failure of the back-up Inertial Reference System followed immediately by failure of the active Inertial Reference System;
- swivelling into the extreme position of the nozzles of the two solid boosters and, slightly later, of the Vulcain engine, causing the launcher to veer abruptly;

- self-destruction of the launcher correctly triggered by rupture of the links between the solid boosters and the core stage.

The origin of the failure was thus rapidly narrowed down to the flight control system and more particularly to the Inertial Reference Systems, which obviously ceased to function almost simultaneously at around H0 + 36.7 seconds.

1.2 INFORMATION AVAILABLE

The information available on the launch includes:

- telemetry data received on the ground until H0 + 42 seconds
- trajectory data from radar stations
- optical observations (IR camera, films) - inspection of recovered material.

The whole of the telemetry data received in Kourou was transferred to CNES/Toulouse where the data were converted into parameter over time plots. CNES provided a copy of the data to Aerospatiale, which carried out analyses concentrating mainly on the data concerning the electrical system.

1.3 RECOVERY OF MATERIAL

The self-destruction of the launcher occurred near to the launch pad, at an altitude of approximately 4000 m. Therefore, all the launcher debris fell back onto the ground, scattered over an area of approximately 12 km2 east of the launch pad. Recovery of material proved difficult, however, since this area is nearly all mangrove swamp or savanna.

Nevertheless, it was possible to retrieve from the debris the two Inertial Reference Systems. Of particular interest was the one which had worked in active mode and stopped functioning last, and for which, therefore, certain information was not available in the telemetry data (provision for transmission to ground of this information was confined to whichever of the two units might fail first). The results of the examination of this unit were very helpful to the analysis of the failure sequence.

1.4 UNRELATED ANOMALIES OBSERVED

Post-flight analysis of telemetry has shown a number of anomalies which have been reported to the Board. They are mostly of minor significance and such as to be expected on a demonstration flight.

One anomaly which was brought to the particular attention of the Board was the gradual development, starting at Ho + 22 seconds, of variations in the hydraulic pressure of the actuators of the main engine nozzle. These variations had a frequency of approximately 10 Hz.

There are some preliminary explanations as to the cause of these variations, which are now under investigation.

After consideration, the Board has formed the opinion that this anomaly, while significant, has no bearing on the failure of Ariane 501.

2. ANALYSIS OF THE FAILURE

2.1 CHAIN OF TECHNICAL EVENTS

In general terms, the Flight Control System of the Ariane 5 is of a standard design. The attitude of the launcher and its movements in space are measured by an Inertial Reference System (SRI). It has its own internal computer, in which angles and velocities are calculated on the basis of information from a "strap-down" inertial platform, with laser gyros and accelerometers. The data from the SRI are transmitted through the databus to the On-Board Computer (OBC), which executes the flight program and controls the nozzles of the solid boosters and the Vulcain cryogenic engine, via servovalves and hydraulic actuators.

In order to improve reliability there is considerable redundancy at equipment level. There are two SRIs operating in parallel, with identical hardware and software. One SRI is active and one is in "hot" stand-by, and if the OBC detects that the active SRI has failed it immediately switches to the other one, provided that this unit is functioning properly. Likewise there are two OBCs, and a number of other units in the Flight Control System are also duplicated.

The design of the Ariane 5 SRI is practically the same as that of an SRI which is presently used on Ariane 4, particularly as regards the software.

Based on the extensive documentation and data on the Ariane 501 failure made available to the Board, the following chain of events, their inter-relations and causes have been established, starting with the destruction of the launcher and tracing back in time towards the primary cause.

- The launcher started to disintegrate at about H0 + 39 seconds because of high aerodynamic loads due to an angle of attack of more than 20 degrees that led to separation of the boosters from the main stage, in turn triggering the self-destruct system of the launcher.
- This angle of attack was caused by full nozzle deflections of the solid boosters and the Vulcain main engine.
- These nozzle deflections were commanded by the On-Board Computer (OBC) software on the basis of data transmitted by the active Inertial Reference System (SRI 2). Part of these data at that time did not contain proper flight data, but showed a diagnostic bit pattern of the computer of the SRI 2, which was interpreted as flight data.
- The reason why the active SRI 2 did not send correct attitude data was that the unit had declared a failure due to a software exception.
- The OBC could not switch to the back-up SRI 1 because that unit had already ceased to function during the previous data cycle (72 milliseconds period) for the same reason as SRI 2.
- The internal SRI software exception was caused during execution of a data conversion from 64-bit floating point to 16-bit signed integer value. The floating point number which was converted had a value greater than what could be represented by a 16-bit signed integer. This resulted in an Operand Error. The data conversion instructions (in Ada code) were not protected from causing an Operand Error, although other conversions of comparable variables in the same place in the code were protected.
- The error occurred in a part of the software that only performs alignment of the strap-down inertial platform. This software module computes meaningful results only before lift-off. As soon as the launcher lifts off, this function serves no purpose.
- The alignment function is operative for 50 seconds after starting of the Flight Mode of the SRIs which occurs at H0 - 3 seconds for Ariane 5. Consequently, when lift-off occurs, the function continues for approx. 40 seconds of flight. This time sequence is based on a requirement of Ariane

4 and is not required for Ariane 5.

- The Operand Error occurred due to an unexpected high value of an internal alignment function result called BH, Horizontal Bias, related to the horizontal velocity sensed by the platform. This value is calculated as an indicator for alignment precision over time.
- The value of BH was much higher than expected because the early part of the trajectory of Ariane 5 differs from that of Ariane 4 and results in considerably higher horizontal velocity values.

The SRI internal events that led to the failure have been reproduced by simulation calculations. Furthermore, both SRIs were recovered during the Board's investigation and the failure context was precisely determined from memory readouts. In addition, the Board has examined the software code which was shown to be consistent with the failure scenario. The results of these examinations are documented in the Technical Report.

Therefore, it is established beyond reasonable doubt that the chain of events set out above reflects the technical causes of the failure of Ariane 501.

2.2 COMMENTS ON THE FAILURE SCENARIO

In the failure scenario, the primary technical causes are the Operand Error when converting the horizontal bias variable BH, and the lack of protection of this conversion which caused the SRI computer to stop.

It has been stated to the Board that not all the conversions were protected because a maximum workload target of 80% had been set for the SRI computer. To determine the vulnerability of unprotected code, an analysis was performed on every operation which could give rise to an exception, including an Operand Error. In particular, the conversion of floating point values to integers was analysed and operations involving seven variables were at risk of leading to an Operand Error. This led to protection being added to four of the variables, evidence of which appears in the Ada code. However, three of the variables were left unprotected. No reference to justification of this decision was found directly in the source code. Given the large amount of documentation associated with any industrial application, the assumption, although agreed, was essentially obscured, though not deliberately, from any external review.

The reason for the three remaining variables, including the one denoting horizontal bias, being unprotected was that further reasoning indicated that they were either physically limited or that there was a large margin of safety, a reasoning which in the case of the variable BH turned out to be faulty. It is important to note that the decision to protect certain variables but not others was taken jointly by project partners at several contractual levels.

There is no evidence that any trajectory data were used to analyse the behaviour of the unprotected variables, and it is even more important to note that it was jointly agreed not to include the Ariane 5 trajectory data in the SRI requirements and specification.

Although the source of the Operand Error has been identified, this in itself did not cause the mission to fail. The specification of the exception-handling mechanism also contributed to the failure. In the event of any kind of exception, the system specification stated that: the failure should be indicated on the databus, the failure context should be stored in an EEPROM memory (which was recovered and read out for Ariane 501), and finally, the SRI processor should be shut down.

It was the decision to cease the processor operation which finally proved fatal. Restart is not feasible since attitude is too difficult to re-calculate after a processor shutdown; therefore the Inertial Reference System becomes useless. The reason behind this drastic action lies in the culture within the Ariane programme of only addressing random hardware failures. From this point of view exception - or error - handling mechanisms are designed for a random hardware failure which can quite rationally be handled by a backup system.

Although the failure was due to a systematic software design error, mechanisms can be introduced to mitigate this type of problem. For example the computers within the SRIs could have continued to provide their best estimates of the required attitude information. There is reason for concern that a software exception should be allowed, or even required, to cause a processor to halt while handling mission-critical equipment. Indeed, the loss of a proper software function is hazardous because the same software runs in both SRI units. In the case of Ariane 501, this resulted in the switch-off of two still healthy critical units of equipment.

The original requirement acccounting for the continued operation of the alignment software after lift-off was brought forward more than 10 years ago for the earlier models of Ariane, in order to cope with the rather unlikely event of a hold in the count-down e.g. between - 9 seconds, when flight mode starts in the SRI of Ariane 4, and - 5 seconds when certain events are initiated in the launcher which take several hours to reset. The period selected for this continued alignment operation, 50 seconds after the start of flight mode, was based on the time needed for the ground equipment to resume full control of the launcher in the event of a hold.

This special feature made it possible with the earlier versions of Ariane, to restart the count- down without waiting for normal alignment, which takes 45 minutes or more, so that a short launch window could still be used. In fact, this feature was used once, in 1989 on Flight 33.

The same requirement does not apply to Ariane 5, which has a different preparation sequence and it was maintained for commonality reasons, presumably based on the view that, unless proven necessary, it was not wise to make changes in software which worked well on Ariane 4.

Even in those cases where the requirement is found to be still valid, it is questionable for the alignment function to be operating after the launcher has lifted off. Alignment of mechanical and laser strap-down platforms involves complex mathematical filter functions to properly align the x-axis to the gravity axis and to find north direction from Earth rotation sensing. The assumption of preflight alignment is that the launcher is positioned at a known and fixed position. Therefore, the alignment function is totally disrupted when performed during flight, because the measured movements of the launcher are interpreted as sensor offsets and other coefficients characterising sensor behaviour.

Returning to the software error, the Board wishes to point out that software is an expression of a highly detailed design and does not fail in the same sense as a mechanical system. Furthermore software is flexible and expressive and thus encourages highly demanding requirements, which in turn lead to complex implementations which are difficult to assess.

An underlying theme in the development of Ariane 5 is the bias towards the mitigation of random failure. The supplier of the SRI was only following the specification given to it, which stipulated that in the event of any detected exception the processor was to be stopped. The exception which occurred was not due to random failure but a design error. The exception was detected, but inappropriately handled because the view had been taken that software should be considered correct until it is shown to be at fault. The Board has reason to believe that this view is also accepted in other areas of Ariane 5 software design. The Board is in favour of the opposite view, that software should be assumed to be faulty until applying the currently accepted best practice methods can demonstrate that it is correct.

This means that critical software - in the sense that failure of the software puts the mission at risk - must be identified at a very detailed level, that exceptional behaviour must be confined, and that a reasonable back-up policy must take software failures into account.

2.3 THE TESTING AND QUALIFICATION PROCEDURES

The Flight Control System qualification for Ariane 5 follows a standard procedure and is performed at the following levels :

- Equipment qualification
- Software qualification (On-Board Computer software)
- Stage integration
- System validation tests.

The logic applied is to check at each level what could not be achieved at the previous level, thus eventually providing complete test coverage of each sub-system and of the integrated system.

Testing at equipment level was in the case of the SRI conducted rigorously with regard to all environmental factors and in fact beyond what was expected for Ariane 5. However, no test was performed to verify that the SRI would behave correctly when being subjected to the count-down and flight time sequence and the trajectory of Ariane 5.

It should be noted that for reasons of physical law, it is not feasible to test the SRI as a "black box" in the flight environment, unless one makes a completely realistic flight test, but it is possible to do ground testing by injecting simulated accelerometric signals in accordance with predicted flight parameters, while also using a turntable to simulate launcher angular movements. Had such a test been performed by the supplier or as part of the acceptance test, the failure mechanism would have been exposed.

The main explanation for the absence of this test has already been mentioned above, i.e. the SRI specification (which is supposed to be a requirements document for the SRI) does not contain the Ariane 5 trajectory data as a functional requirement.

The Board has also noted that the systems specification of the SRI does not indicate operational restrictions that emerge from the chosen implementation. Such a declaration of limitation, which should be mandatory for every mission-critical device, would have served to identify any non-compliance with the trajectory of Ariane 5.

The other principal opportunity to detect the failure mechanism beforehand was during the numerous tests and simulations carried out at the Functional Simulation Facility ISF, which is at the site of the Industrial Architect. The scope of the ISF testing is to qualify :

- the guidance, navigation and control performance in the whole flight envelope,
- the sensors redundancy operation, - the dedicated functions of the stages,

- the flight software (On-Board Computer) compliance with all equipment of the Flight Control Electrical System.

A large number of closed-loop simulations of the complete flight simulating ground segment operation, telemetry flow and launcher dynamics were run in order to verify :

- the nominal trajectory
- trajectories degraded with respect to internal launcher parameters
- trajectories degraded with respect to atmospheric parameters
- equipment failures and the subsequent failure isolation and recovery

In these tests many equipment items were physically present and exercised but not the two SRIs, which were simulated by specifically developed software modules. Some open-loop tests, to verify compliance of the On-Board Computer and the SRI, were performed with the actual SRI. It is understood that these were just electrical integration tests and "low-level " (bus communication) compliance tests.

It is not mandatory, even if preferable, that all the parts of the subsystem are present in all the tests at a given level. Sometimes this is not physically possible or it is not possible to exercise them completely or in a representative way. In these cases it is logical to replace them with simulators but only after a careful check that the previous test levels have covered the scope completely.

This procedure is especially important for the final system test before the system is operationally used (the tests performed on the 501 launcher itself are not addressed here since they are not specific to the Flight Control Electrical System qualification).

In order to understand the explanations given for the decision not to have the SRIs in the closed-loop simulation, it is necessary to describe the test configurations that might have been used.

Because it is not possible to simulate the large linear accelerations of the launcher in all three axes on a test bench (as discussed above), there are two ways to put the SRI in the loop:

A) To put it on a three-axis dynamic table (to stimulate the Ring Laser Gyros) and to substitute the analog output of the accelerometers (which can not be stimulated mechanically) by simulation via a dedicated test input connector and an electronic board designed for this purpose. This is similar to the method mentioned in connection with possible testing at equipment level.

B) To substitute both, the analog output of the accelerometers and the Ring Laser Gyros via a dedicated test input connector with signals produced by simulation.

The first approach is likely to provide an accurate simulation (within the limits of the three-axis dynamic table bandwidth) and is quite expensive; the second is cheaper and its performance depends essentially on the accuracy of the simulation. In both cases a large part of the electronics and the complete software are tested in the real operating environment.

When the project test philosophy was defined, the importance of having the SRIs in the loop was recognized and a decision was taken to select method B above. At a later stage of the programme (in 1992), this decision was changed. It was decided not to have the actual SRIs in the loop for the following reasons :

- The SRIs should be considered to be fully qualified at equipment level
- The precision of the navigation software in the On-Board Computer depends critically on the precision of the SRI measurements. In the ISF, this precision could not be achieved by the electronics creating the test signals.
- The simulation of failure modes is not possible with real equipment, but only with a model.
- The base period of the SRI is 1 millisecond whilst that of the simulation at the ISF is 6 milliseconds. This adds to the complexity of the interfacing electronics and may further reduce the precision of the simulation.

The opinion of the Board is that these arguments were technically valid, but since the purpose of a system simulation test is not only to verify the interfaces but also to verify the system as a whole for the particular application, there was a definite risk in assuming that critical equipment such as the SRI had been validated by qualification on its own, or by previous use on Ariane 4.

While high accuracy of a simulation is desirable, in the ISF system tests it is clearly better to compromise on accuracy but achieve all other objectives, amongst them to prove the proper system integration of equipment such as the SRI. The precision of the guidance system can be effectively demonstrated by analysis and computer simulation.

Under this heading it should be noted finally that the overriding means of preventing failures are the reviews which are an integral part of the design and qualification process, and which are carried out at all levels and involve all major partners in the project (as well as external experts). In a programme of this size, literally thousands of problems and potential failures are successfully handled in the review process and it is obviously not easy to detect software design errors of the type which were the primary technical cause of the 501 failure. Nevertheless, it is evident that the limitations of the SRI software were not fully analysed in the reviews, and it was not realised that the test coverage was inadequate to expose such limitations. Nor were the possible implications of allowing the alignment software to operate during flight realised. In these respects, the review process was a contributory factor in the failure.

2.4 POSSIBLE OTHER WEAKNESSES OF SYSTEMS INVOLVED

In accordance with its termes of reference, the Board has examined possible other weaknesses, primarily in the Flight Control System. No weaknesses were found which were related to the failure, but in spite of the short time available, the Board has conducted an extensive review of the Flight Control System based on experience gained during the failure analysis.

The review has covered the following areas :

- The design of the electrical system,
- Embedded on-board software in subsystems other than the Inertial Reference System,
- The On-Board Computer and the flight program software.

In addition, the Board has made an analysis of methods applied in the development programme, in particular as regards software development methodology.

The results of these efforts have been documented in the Technical Report and it is the hope of the Board that they will contribute to further improvement of the Ariane 5 Flight Control System and its software.

3. CONCLUSIONS

3.1 FINDINGS

The Board reached the following findings:

a) During the launch preparation campaign and the count-down no events occurred which were related to the failure.

b) The meteorological conditions at the time of the launch were acceptable and did not play any part in the failure. No other external factors have been found to be of relevance.

c) Engine ignition and lift-off were essentially nominal and the environmental effects (noise and vibration) on the launcher and the payload were not found to be relevant to the failure. Propulsion performance was within specification.

d) 22 seconds after H0 (command for main cryogenic engine ignition), variations of 10 Hz frequency started to appear in the hydraulic pressure of the actuators which control the nozzle of the main engine. This phenomenon is significant and has not yet been fully explained, but after consideration it has not been found relevant to the failure.

e) At 36.7 seconds after H0 (approx. 30 seconds after lift-off) the computer within the back-up inertial reference system, which was working on stand-by for guidance and attitude control, became inoperative. This was caused by an internal variable related to the horizontal velocity of the launcher exceeding a limit which existed in the software of this computer.

f) Approx. 0.05 seconds later the active inertial reference system, identical to the back-up system in hardware and software, failed for the same reason. Since the back-up inertial system was already inoperative, correct guidance and attitude information could no longer be obtained and loss of the mission was inevitable.

g) As a result of its failure, the active inertial reference system transmitted essentially diagnostic information to the launcher's main computer, where it was interpreted as flight data and used for flight control calculations.

h) On the basis of those calculations the main computer commanded the booster nozzles, and somewhat later the main engine nozzle also, to make a large correction for an attitude deviation that had not occurred.

i) A rapid change of attitude occurred which caused the launcher to disintegrate at 39 seconds after H0 due to aerodynamic forces.

j) Destruction was automatically initiated upon disintegration, as designed, at an altitude of 4 km and a distance of 1 km from the launch pad.

k) The debris was spread over an area of 5 x 2.5 km2. Amongst the equipment recovered were the two inertial reference systems. They have been used for analysis.

l) The post-flight analysis of telemetry data has listed a number of additional anomalies which are being investigated but are not considered significant to the failure.

m) The inertial reference system of Ariane 5 is essentially common to a system which is presently flying on Ariane 4. The part of the software which caused the interruption in the inertial system computers is used before launch to align the inertial reference system and, in Ariane 4, also to enable a rapid realignment of the system in case of a late hold in the countdown. This realignment function, which does not serve any purpose on Ariane 5, was nevertheless retained for commonality reasons and allowed, as in Ariane 4, to operate for approx. 40 seconds after lift-off.

n) During design of the software of the inertial reference system used for Ariane 4 and Ariane 5, a decision was taken that it was not necessary to protect the inertial system computer from being made inoperative by an excessive value of the variable related to the horizontal velocity, a protection which was provided for several other variables of the alignment software. When taking this design decision, it was not analysed or fully understood which values this particular variable might assume when the alignment software was allowed to operate after lift-off.

o) In Ariane 4 flights using the same type of inertial reference system there has been no such failure because the trajectory during the first 40 seconds of flight is such that the particular variable related to horizontal velocity cannot reach, with an adequate operational margin, a value beyond the limit present in the software.

p) Ariane 5 has a high initial acceleration and a trajectory which leads to a build-up of horizontal velocity which is five times more rapid than for Ariane 4. The higher horizontal velocity of Ariane 5 generated, within the 40-second timeframe, the excessive value which caused the inertial system computers to cease operation.

q) The purpose of the review process, which involves all major partners in the Ariane 5 programme, is to validate design decisions and to obtain flight qualification. In this process, the limitations of the alignment software were not fully analysed and the possible implications of allowing it to continue to function during flight were not realised.

r) The specification of the inertial reference system and the tests performed at equipment level did not specifically include the Ariane 5 trajectory data. Consequently the realignment function was not tested under simulated Ariane 5 flight conditions, and the design error was not discovered.

s) It would have been technically feasible to include almost the entire inertial reference system in the overall system simulations which were performed. For a number of reasons it was decided to use the simulated output of the inertial reference system, not the system itself or its detailed simulation. Had the system been included, the failure could have been detected.

t) Post-flight simulations have been carried out on a computer with software of the inertial reference system and with a simulated environment, including the actual trajectory data from the Ariane 501 flight. These simulations have faithfully reproduced the chain of events leading to the failure of the inertial reference systems.

3.2 CAUSE OF THE FAILURE

The failure of the Ariane 501 was caused by the complete loss of guidance and attitude information 37 seconds after start of the main engine ignition sequence (30 seconds after lift- off). This loss of information was due to specification and design errors in the software of the inertial reference system.

The extensive reviews and tests carried out during the Ariane 5 Development Programme did not include adequate analysis and testing of the inertial reference system or of the complete flight control system, which could have detected the potential failure.

4. RECOMMENDATIONS

On the basis of its analyses and conclusions, the Board makes the following recommendations.

R1 Switch off the alignment function of the inertial reference system immediately after lift-off. More generally, no software function should run during flight unless it is needed.

R2 Prepare a test facility including as much real equipment as technically feasible, inject realistic input data, and perform complete, closed-loop, system testing. Complete simulations must take place before any mission. A high test coverage has to be obtained.

R3 Do not allow any sensor, such as the inertial reference system, to stop sending best effort data.

R4 Organize, for each item of equipment incorporating software, a specific software qualification review. The Industrial Architect shall take part in these reviews and report on complete system testing performed with the equipment. All restrictions on use of the equipment shall be made explicit for the Review Board. Make all critical software a Configuration Controlled Item (CCI).

R5 Review all flight software (including embedded software), and in particular :

- Identify all implicit assumptions made by the code and its justification documents on the values of quantities provided by the equipment. Check these assumptions against the restrictions on use of the equipment.
- Verify the range of values taken by any internal or communication variables in the software.
- Solutions to potential problems in the on-board computer software, paying particular attention to on-board computer switch over, shall be proposed by the project team and reviewed by a group of external experts, who shall report to the on-board computer Qualification Board.

R6 Wherever technically feasible, consider confining exceptions to tasks and devise backup capabilities.

R7 Provide more data to the telemetry upon failure of any component, so that recovering equipment will be less essential.

R8 Reconsider the definition of critical components, taking failures of software origin into account (particularly single point failures).

R9 Include external (to the project) participants when reviewing specifications, code and justification documents. Make sure that these reviews consider the substance of arguments, rather than check that verifications have been made.

R10 Include trajectory data in specifications and test requirements.

R11 Review the test coverage of existing equipment and extend it where it is deemed necessary.

R12 Give the justification documents the same attention as code. Improve the technique for keeping code and its justifications consistent.

R13 Set up a team that will prepare the procedure for qualifying software, propose stringent rules for confirming such qualification, and ascertain that specification, verification and testing of software are of a consistently high quality in the Ariane 5 programme. Including external RAMS experts is to be considered.

R14 A more transparent organisation of the cooperation among the partners in the Ariane 5 programme must be considered. Close engineering cooperation, with clear cut authority and responsibility, is needed to achieve system coherence, with simple and clear interfaces between partners.

- END -