CASE STUDY NO: 6 - ARIANE 5 FAILURE

20VV1A1263

March 31, 2022

1 Introduction:

This case study describes the accident that occurred on the initial launch of the Ariane 5 rocket, a launcher developed by the European Space Agency. The rocket exploded shortly after take-off and the subsequent enquiry showed that this was due to a fault in the software in the inertial navigation system.

In June 1996, the then new Ariane 5 rocket was launched on its maiden flight. It carried a payload of scientific satellites. Ariane 5 was commercially very significant for the European Space Agency as it could carry a much heavier payload than the Ariane 4 series of launchers. Thirty seven seconds into the flight, software in the inertial navigation system, whose software was reused from Ariane 4, shut down causing incorrect signals to be sent to the engines. These swivelled in such a way that uncontrollable stresses were placed on the rocket and it started to break up. Ground controllers initiated self-destruct and the rocket and payload was destroyed.

A subsequent enquiry showed that the cause of the failure was that the software in the inertial reference system shut itself down because of an unhandled numeric exception (integer overflow). There was a backup software system but this was not diverse so it failed in the same way.

2 Elaborating the event:

2.1 1. THE FAILURE

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.

2.2 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.

2.3 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.

2.4 ANALYSIS OF THE FAILURE

2.5 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.

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 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 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.

2.6 POSSIBLE OTHER WEAKNESSES OF SYSTEMS INVOLVED

LaTeX 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.

2.7 CONCLUSIONS:

2.8 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.

2.9 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.

2.10 Lessons Learnt:

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.

2.11 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

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.