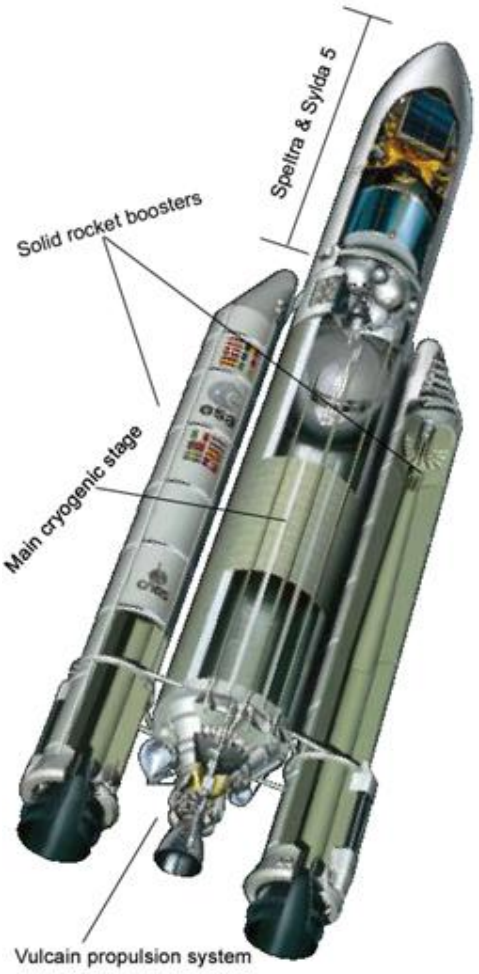
ariane 5

Chronicle of a Failure

Contents:

Introduction - Abstract

Nowadays the space missions are in the centre of attention. The last four decades space programs have kept evolving constantly. Such a space program is the Ariane 5. The Ariane 5 is a space rocket that was constructed to transfer space shuttles to orbit. Before starting investigating the various concepts of the failure of the Ariane 5 (flight 501) mission we must distinguish some basic terms. In the following diagram we can see clearly the parts that the flight 501 consists of.



Ariane 5 is the designation of the rocket that is used to send a space shuttle in orbit.

The space shuttle in the case of the flight 501 was called Speltra & Sylda 5. The cause was to serve communications needs. The space shuttle was unmanned.

Different space shuttles are sending in orbit to serve different needs but a specific version of the rocket can be used many times. Ariane 5 was the latest version of a rocket series from Ariane 1 - 4.

The Ariane 5 rocket construction consists of three basic parts, the main cryogenic stage, the solid rocket boosters and the Vulcain propulsion system.

Ariane 5 also used successfully to carry out to space the magnificent well-known Habble endeavor telescope.

The Ariane 5 European Space Agency (ESA) rocket was ready for launch on the morning of 4 June 1996 with a price tag of US$500 million. After a small delay due to visibility reasons, the launch was successful. Nominal behaviour of the launcher was observed up to H0 + 36 seconds. Failure of the back-up Inertial Reference System followed immediately by failure of the active Inertial Reference System.

This caused swivelling into the extreme position of the nozzles of the two solid boosters and seconds later, of the Vulcain engine, causing the launcher to veer off its flight path. This resulted in self-destruction of the launcher which was correctly

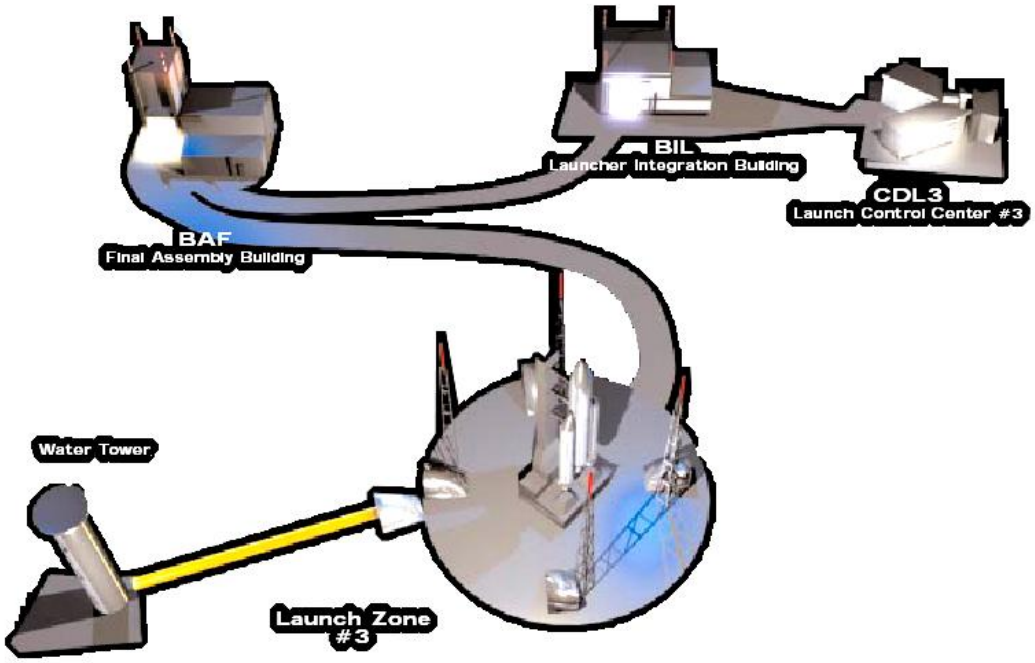
triggered – according to specifications -by rupture of the links between the solid boosters and the core stage.

This report, based on all available publication, will attempt recount the events as the transpired leading to the disaster and analyse the main contributors and causes that lead to that disaster. Will proceed with a critical analysis of the standards employed, and critically review the Risk and Hazard analysis and its impact on the failure. It will conclude by discussing any legal or ethical issues and the consequences on the involved parties.

4.1.0 Factual Background

In this section we will recount the events as the happened without providing any explanation as to what caused them. Later on, in the second chapter we will provide and analyse the cause for each and every one of them and eventually will draw the necessary conclusions as to what was the real cause.

The weather at the launch site at Kourou, French Guinea, was acceptable for a launch that day, and presented no obstacle to the transfer of the launcher to the launch pad.



Ariane 5 (flight 501) route 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 concern was the fulfilment of the visibility criteria.

Visibility dropped even further, resulting in the countdown to halt at H0-7 minutes. At that time it was decided that the visibility criteria were not met for the predetermined launch window on 08h35 local time.
Visibility conditions improved as forecast and the launch was initiated at H0[1] = 09h 33mn 59s local time (12h 33mn 59s UT).

At H0 full system diagnostics on:

1. Main cryogenic stage
2. Vehicle Equipment Bay (VEB)
3. Upper stage - fairing - SPELTRA - payload adapters
4. Electrical system
5. Ground-to-launcher interface - lift-off - trajectory
6. Flight control
7. Aerothermodynamics - depressurisation - air cleanliness

was successful – the above list is defined in all space travel standards.

Ignition of the Vulcain engine and the two solid boosters was nominal, and so was lift-off. Propulsion performance was within specification.

After 22 seconds from H0 (time scheduled for 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.

At 36.7 seconds after lift off 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.

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.

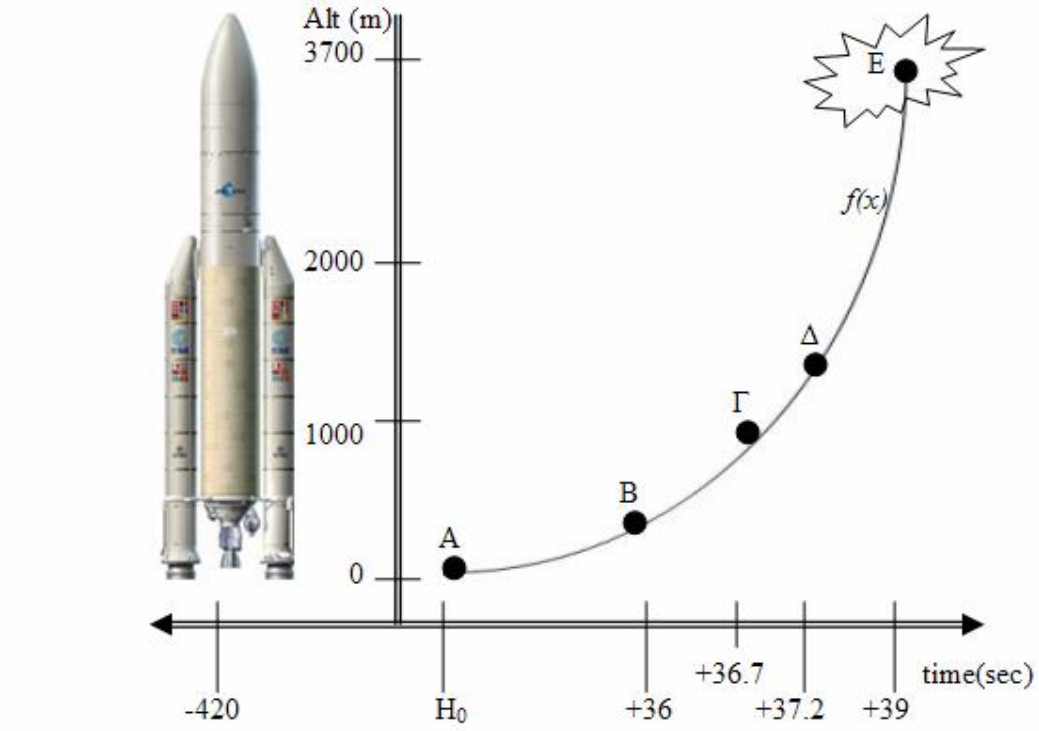
A rapid change of attitude occurred which caused the launcher to disintegrate at 39 seconds after H0 due to aerodynamic forces.

[1] H_0 **à** Hour 0 (zero): relative representation of the ignition time.

Destruction was automatically initiated upon disintegration, as designed, at an altitude of 3700 m and a distance of 1 km from the launch pad.

A QuickTime format video of the incident is available at:
http://www2.vuw.ac.nz/staff/stephen_marshall/SE/Failures/media/Ariane.mov
which represents a more pictorial description of the events as told above.

A graphical representation was designed from the authors of this report and is given below in order to help us understand the incident. Also we can see the mathematical interrelation representing the parabolic equation of the launcher's speed [*f(x)*].



$f(x)=ax^2+bx+c,\ a<>0$

Explaining the above diagram we can see clearly that at the H_0 – 7 minutes (-420 seconds) point the rocket was placed successfully to the launch pad. In basic terms these are the five stages that the rocket was until the explosion.

A) In altitude zero meters and the time H_0 the launce sequence has started and after 9 second we had a successful lift off.

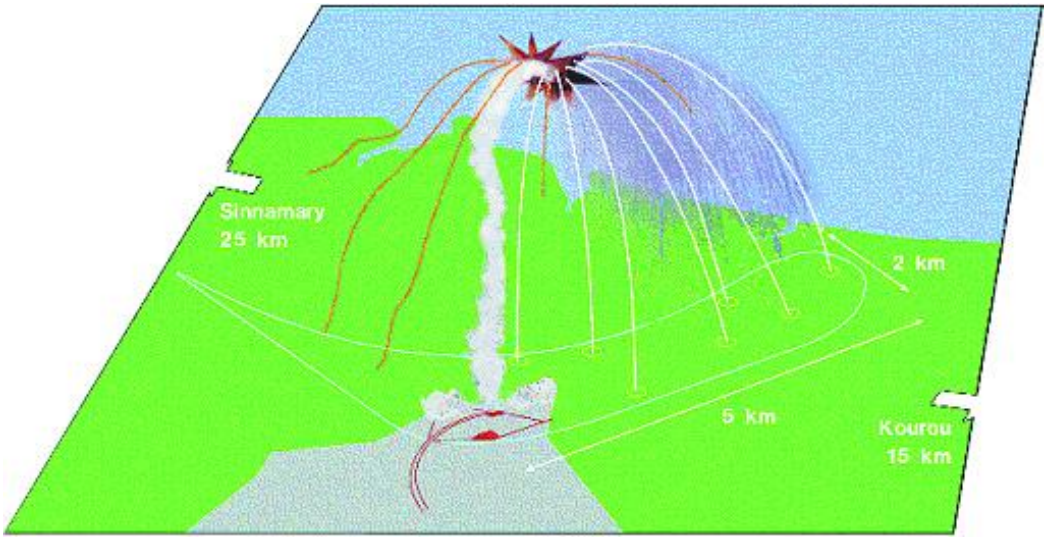
B) A nominal behaviour of the rocket until that time.

Γ) Failure of the back-up inertial reference system followed immediately by failure of the active inertial reference system.

Δ) Swiveling 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.

E) Self – destruction of the launcher correctly triggered by rupture of the links between the solid boosters and the core stage (Altitude 3700m.).

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



Fragment fallout zone (Source: CNES/CSG)

All the launcher debris fell back onto the ground, scattered over an area of approximately 12 km2 east of the launch pad. The recovery of the debris was proven a difficult task for the agency since nearly all mangrove swamp or savannah.

Fragment-recovery operations were started immediately thereafter and involved almost one hundred people (safety engineers and technicians, firemen, security guards, and legionnaires) over a period of several weeks. Helicopters and special amphibious vehicles were deployed.

Amongst other debris, discovered was the two Inertial Reference Systems. The search teams were specifically instructed to recover the second IRS unit which had worked in active mode and stopped functioning last. This interest is justified from the fact that

certain information was not available in the telemetry data since provision for transmission to ground of this information was confined to whichever of the two units might fail first.

Other available data except from the recovery of the debris were telemetry data received on the ground until H0 + 42 seconds. Also trajectory data from radar stations and optical observations (IR camera, films).

Post-flight analysis of telemetry has shown a number of anomalies which have been reported but they were justly dismissed as of minor significance and such as to be expected on a demonstration flight.

4.2.0 Analysis – Main contributors - Causes

In the next lines we will approach more technical characteristics that characterise the ARIANE 5. As we have mentioned before, ARIANE 5 is the name of the part that provides the booster force.

The system of the flight control is standard design and the locomotion in space is measured by a system that is named SRI (Inertial Reference System). Also exists an internal computer where the angles and the velocities are calculated according the information that comes from the "strap –down" inertial platform. The inertial platform is composed from laser gyros and accelerometers. The SRI system sends all the information that collects in the central computer of the shuttle OBC (On –Board Computer) aiming their processing. Then, the central computer executes the flight program. The OBC using servo valves and hydraulic actuators controls the nozzles of the solid boosters and the Vulcain.

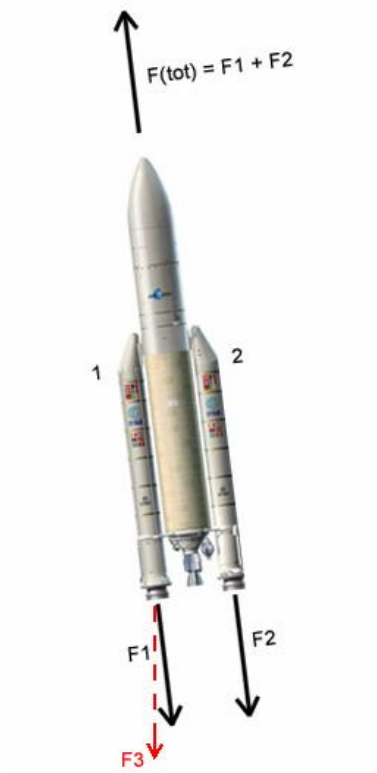
There are two SRI on the contraction. The two SRIs operating in parallel and they are controlled by the same software and hardware. The first SRI is active and is responsible for the flight. The second SRI is in "hot stand – by" in case the first fails. The OBC detects continuously the state of the SRIs. In case the OBC detect a problem with the first SRI switches immediately to the second knowing that the second is working properly. Of course there are two OBC and many more flight control units in duplicates.

When the backup SRI failed on ARINE 5 the rocket has no problem to continue its flight but almost immediately the main SRI failed and there was no backup system stand by anymore. Part of these data at that time was not actually proper flight data, but showed a diagnostic bit pattern of the computer of the SRI 2, which was interpreted as flight data. That's when the rocket lost completely the guidance system. The OBC was using the servo valve and the hydraulic actuators without valid input. This had as result the incoercible and wrong boosting power to the rocket.

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

The erroneous data has interpreted as flight data by the active SRI. The SRI unit had declared a failure due to a software exception.

The OBC could not switch to the back-up SRI because that unit had already ceased to function - according to system specifications - during the previous data cycle (72 milliseconds period) for exactly the same reason as the main SRI.



In the picture we can see the forces applied to the rocket from the solid boosters. The boosters working in parallel provide a total force F (tot) which is equal to the sum of F1 from booster 1 and F2 from booster 2.

If we have wrong boosting power from one of the boosters the total force that moves the rocket changes completely towards the direction of the movement.

The erroneous force on the frame causes the separation of the booster from the main rocket.

In result we have an alternative course and the auto distraction of the rocket is engaged.

Looking the timeline backwards we can trace the events and explain the cause of the disaster. At about H0 + 39 seconds the launcher started to disintegrate 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.

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 causing an overflow error and thus forcing the back-up SRI and consecutively the main SRI to cease function.

The data conversion instructions in Ada, were not protected - in programming terms meaning that no boundary check was done to see whether the 64-bit floating point result of the function could be stored into a 16-bit signed integer variable - 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. After lift-off occurs, the function continues for approximately 40 seconds of flight. This time sequence was however 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 primary technical causes were 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.

4.3.0 Standards Analysis and Critique

A pointer to the full document of the standards used for the Ariane 5 project can be found in the bibliography section. Here we will highlight the strong points in standards documentation while in the following section will criticize their omissions - if any- suggest what could/should have happened.

4.3.1 Positive Contribution Of Standards

Here we will comment and point out the positive contribution of the standards to the overall process as they were revealed after the research undertaken.

Rigorous standards existed at the time the project was initiated and were followed as closely as possible. As stated in the standards document (ref [7]) that were employed for the Ariane 5 project, standardised procedures exist for the following:

- Ø Product Standards, contains standards, recommendations and guidelines concerning the product, i.e. the software to be defined, implemented, operated and maintained.

- Ø Procedure Standards: describes the procedures which are used to manage a software project.

In the same document, when it comes to software verification and approval, formal methods such as Z or VDM are recommended to be used ref [8], which indicates a high standard and commitment.

The ESA and its sub contractor's standards are applied at the following levels - according to the Enquiry Board-:

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

At each level a rigorous check and validation is carried out to establish what could not be achieved at the previous level, so eventually providing complete test coverage of each sub-system and of the integrated system. In their standards there are also detail specifications about testing at every individual stage.

Overall as revealed though the investigation, the strict standards were employed in this project and the failure is not in any way appointed, according to the Enquiry Board, to lack of proper standards.

4.3.2 Standards Shortcoming

While there were rigorous standards at present the project fail due to various shortcomings the existed in their specification. These will be highlighted and discussed below.

Inadequate Testing and Wrong type of reuse:

The Ariane 5 flight profile was not included in the IRS system specification. As a direst consequence IRS contractor did not have the proper data with which to perform a test. Testing with the Ariane 4 flight data would not have violated the assertion ref [6], and thus the error would not have been detected.

No revalidation procedures were determined:
The prime contractor decided against performing these tests, preferring instead to assume that their experience with this IRS on Ariane 4 was sufficient, along with the vendor's qualification tests, to qualify the IRS in the total system.

SQA procedures even though the existed and strictly defined in the standards ref [QA] for ever aspect of software development along with the use of formal methods (validation, assertions etc) there are inevitable questions arising abut the use of the right personnel.

Even if the assertion for that piece of code was properly defined, it would not have provided any benefit if the right personnel did not review the assertion for correctness. The Design by Contract: The Lessons of Ariane by Jean-Marc Jézéquel, IRISA and Bertrand Meyer, ISE appeared in Computer (IEEE), as part of the Object-Oriented department, in January of 1997 (vol. 30, no. 2, pages 129-130) speaks of a "QA team" performing this function. Even though a QA tea was in place according to ESA standards, QA teams, do not always have the experience and knowledge base to determine difficult technical questions.

And this is the case with the QA team operating in this project. It is stated in the ESA standards and methodology used that, the QA team was composed of individuals who are not also responsible for development of the system. Another similar example is the US Department of Defence software standards DoD-STD-2167 and DoD-STD-2168, which were used in the same time-frame as the original Ariane software development.

In safety critical systems today, external validation by independent bodies are brought in to verify and also to provide adequate analysis capabilities. That was not the case in the Ariane 5 project as the failure report suggests [2] and also there is no mention about this procedures in the standards document.

From the research undertaken it is unclear that any team within the subcontractor responsible for the IRS development had the necessary expertise to determine the fault that lie within their system.

This fault was not an internal contradiction within the IRS design. It was a fault in the operation of the IRS within the larger Ariane 5 system ref. [1].

4.4.0 The role of Risk & Hazard Analysis (R&HA) in the System

In this section we will present the main finding of the Risk & Hazard Analysis, which it *was* undertaken - we are not question it's existence but it's effectiveness -, and draw conclusion for the practice of R&HA for that particular project.

Risk and Hazard was a part of the ESA and its sub contractor's standard code of practise. Indeed Risk and Hazard analysis was undertaken for the Ariane 5 flight 501 especially in regards to software and hardware parts of the rocket (see Appendix 2 were we present the risk management project lifecycle and risk estimation as evidence that ESA *did* the technique).

That process defined that not all the conversions were protected because a maximum workload target of 80% had been set for the SRI computer. That was a threshold for the processor as defined by the engineers that would protect the OBC from an overload.

To determine the vulnerability of unprotected code, an analysis was also 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. No evidence of that decision was directly found in the source code documentation according to the Enquiry Board's findings.

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.

Nuseibeh argues [3] that lack of or malpractice of Risk Analysis may explain why the fatal exception was not handled. The primary concern of the development team was to keep the processor workload below the chosen threshold of 80 percent as mentioned above. This was a clear requirement conflict between robustness and processor load which should have been investigating further at the time.

Jézéquel and Meyer [5] in their paper "Design by contract: the lessons of Ariane" - also known as the "Eiffel paper" - have suggested a focus on "design by contract", and propose various solutions for being able to notice such conflicts, such as specifying preconditions and post conditions.

Risk analysis in this project, even though diligently done at the beginning of the project it was the forgotten.

4.5.0 In Retrospect - Recommendations

There was an evident lack of subcontractor's communication .The relationship between the companies was not as efficient as it could have been which was made evident by the suggestions made in the report by the enquiry board ref [1].

After studying the Enquiry Board report it was noted that they refer to the prime contractor as the *"Industrial Architect"*, but does not refer to any of the parties by name.

Rigorous research revealed that in Aviation Week and Space Technology ref [2] ran articles following the incident, in which they identified the IRS supplier as Sextant

and the prime contractor as Arianespace, along with a description of their respective roles. As a result, the IRS vendor might not have had the total expertise base available to properly analyze such an assertion.

A more transparent organisation of the cooperation among the partners in the Ariane 5 programme should have been considered. Close engineering cooperation, with clear cut authority and responsibility, is needed to achieve system coherence, with simple and clear communication protocols between partners in place.

Another thing that should have been defined more rigidly is the use of external reviewers. If external to the project participants, were including in the validation and verification procedures, reviewing specifications, code and justification documents any error is more likely to get caught. The reviews should consider the substance of arguments, rather than just check that verifications have been made.

More details should have been paid to integrated system testing. Integrated system testing at the prime contractor, using the proper test environment and data, would have been able to detect the error.

Stricter software design principles such the principles of Design by Contract should have been employed. Even though, by no means we suggest that a different choice of language, the software was written in Ada, could have changed the course of events, the principles used in such a methodology might have made the error either more evident or would not allowed to happen.

Any software element that has a fundamental constraint should state it explicitly, as part of a mechanism present in the programming language, e.g. in Eiffel.

After the incident, many were criticizing the Ada programming language for being primarily responsible for the Operand error. A “language war” broke out between supporters - and gurus - of Ada and Eiffel. Both views were researched and critically evaluated but even though in the article “The Design by Contract: The Lessons of Ariane” by Jean-Marc Jézéquel, IRISA and Bertrand Meyer, ISE which appeared in Computer (IEEE), as part of the Object-Oriented section makes a good point on the software re use error being the true cause.

It also states that the QA team’s primarily focus should have been the review of the software assertion. As pointed above formal proofs, which *were* used during the project, do not make such a nice reading for QA teams, and for that matter no one that is not a highly skilled qualified engineer. They also propose that Eiffel type assertion could have saved the day which is debatable.

QA teams when appointed they should consist of the proper personnel. Even though engineers might be sometimes biased in criticizing work of other engineers they should not be eliminated from the QA team selection as they provide the necessary technological expertise which are important in judging software quality.

Another matter that we should address here is the fact that, event though the three variable the remained unprotected, and the decision approved by regular channels, and even though there was proper documentation of the assertions for every variable

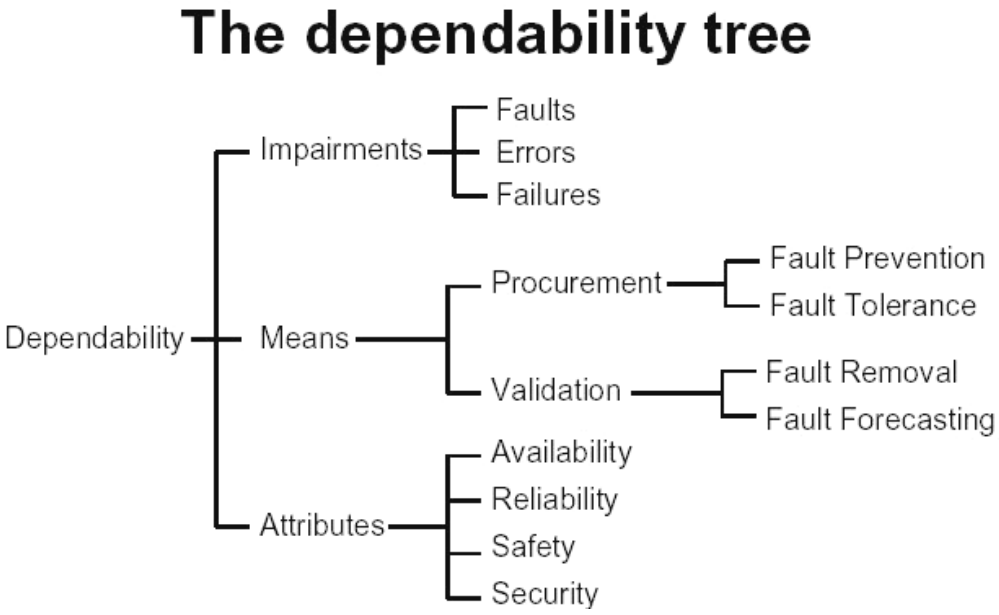
in the documentation, the quality of the documentation and its reviewers should have specific trades that were absent but had they been there the disaster might have been averted:

- The critical assertion should have to be documented (correctly) in the code.
- The review team should have the proper expertise to detect the problem (something not present in the QA team in this project, as proven above).
- The review team should have to review the code, as opposed to other documentation.
- The review team should have to select the critical assertion from the total set of assertions (since if done properly they should have the expertise to do so)
- The review team should have access the proper source information regarding Ariane 5 flight profile to realize that a problem existed.

Finally, a suggestion that could have mad a difference, based on the fact that many pieces of machinery were duplicated aboard the shuttle as a security measure, is that if the second SRI was using a different version of the software used on the first one or even yet a totally different software it could have prevented the disaster.

Possibly a different subcontractor could have been employed to design a different application for the second SRI that would have nothing in common with the first but would still would serve the same purpose.

From the budget point of view, that seems feasible all though we do not really now the time scale and constraints that were imposed on this project. By this suggestion by no means we claim that the disaster could have been averted since the same error could have occurred in both SRIs even of they were constructed by different vendors. But there is a very probability that from two different teams working separately and using different design methodologies, one might have either discover the fatal error in the code or could have protected all variables still maintaining the 80% threshold that was required for the OBC.



Generally if we are to identify the shortcoming in the design methodology using the above diagram as a guide for creating a dependable system, we can make the following remarks:

- Improper Fault Prevention mechanisms
- Absence of Fault Tolerance mechanisms
- Improper Fault Forecasting and testing mechanisms (for reasons explained above)

While the security and safety attributes of the system were high Availability and Reliability were relatively low.

4.6.0 Ethical Issues - Environmental damage

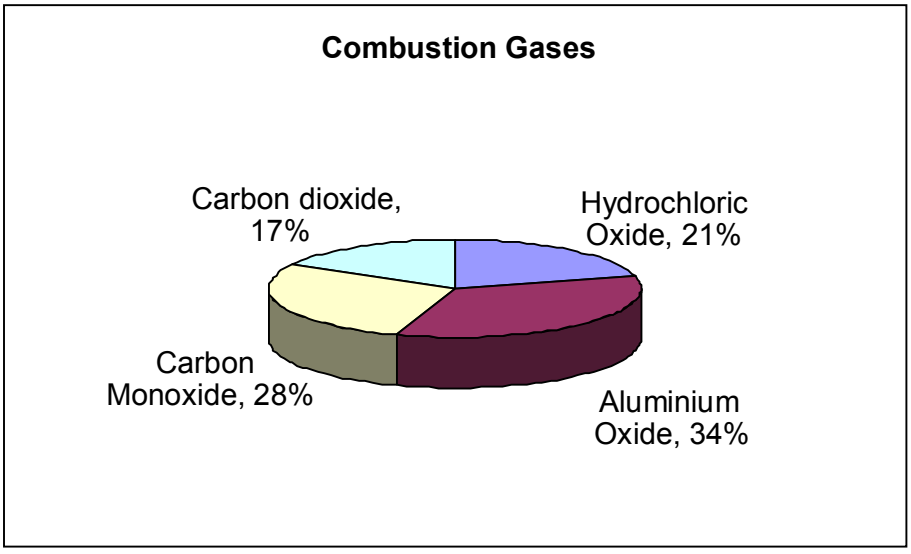
When reporting the Ethical and issues concerning the accident we should make clear that fact that the shuttle was unmanned resulted in no loss of life and hence no legal actions were taken against anyone according to official records.

However, an official enquiry was launched, and its findings included recommendation towards the European Space Agency as to the causes of the failure and future recommendation. After the publication of the enquiry no subcontractors contract's where cancelled or suspended. However a major changes and reviews of standards and practices were applied.

Another issue that followed the accident, an ethical one, was the environmental damage. ESA had well formed plans for such a case.

In order to determine the mathematical models of combustion – cloud dispersion and adjust the chemical fallout several tests took place during 1993 and 1995. According the French and the international regulations applicable to industrial installations, a very detailed risk and impact analysis should performed during the design. Seven booster test firings performed in order to find out the real impact on the natural environment (atmosphere, fauna, flora, and water courses).

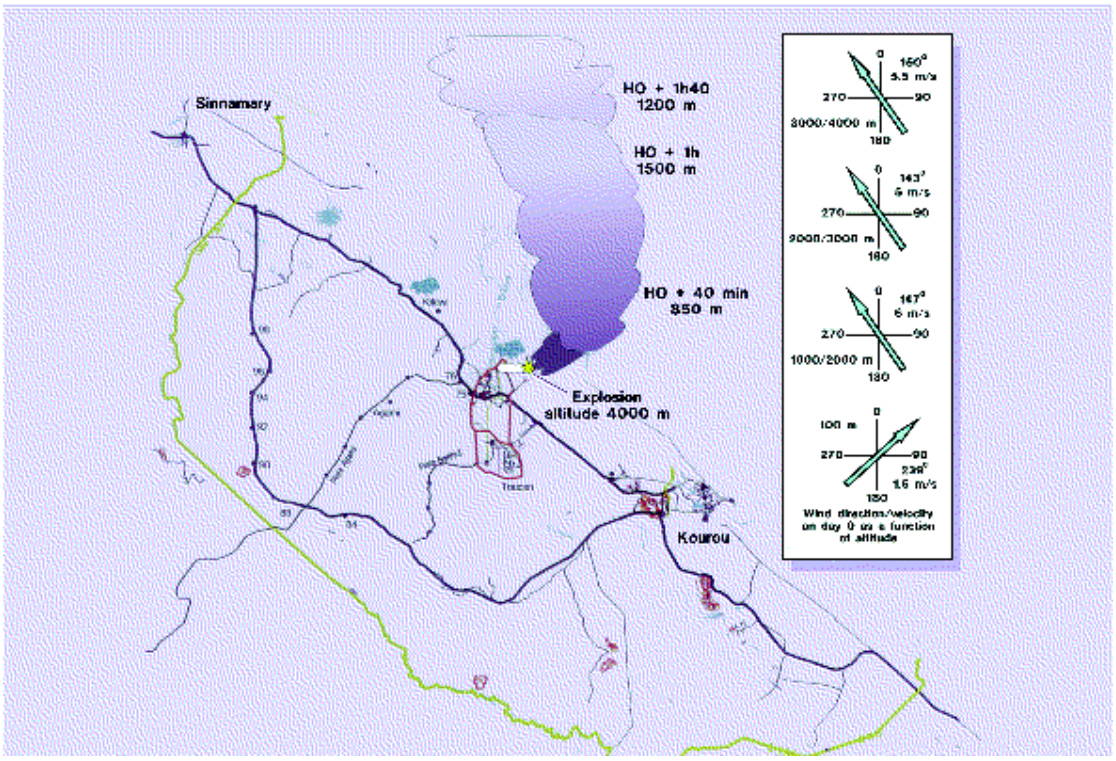
The combustion gases from the solid boosters during the atmospheric flight consist of hydrochloric oxide, aluminium oxide, carbon monoxide and carbon dioxide. The following diagram showing the result of combustion gases into the atmosphere and their percentage.



More than 100 sensors were installed around the launce pad covering a circled area of 25 km for flight 501. The results were showed that a hydrochloric acid and aluminium

oxide fallout occurred within a 500m radius of the launch pad. No gaseous pollution at ground level was detected by any oh the measuring instruments outside the launch area. The helicopter monitoring the gases from the explosion after three hours reported that the gases were moved several kilometres off coast and were dissipating gradually.

The lift – off cloud, some still burning solid – propellant fragments from the boosters and the vaporisation of the launcher where tried to be monitored at ground level also. These gases where also headed to the see at an altitude of more than 1000m.



Explosion Gasses as spread in atmosphere and their spread over time (Source: CNES/CSG)

4.7.0 – References, Bibliography and Web Bibliography

References:

[1] *"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 time-frame, the excessive value [BH] which caused the inertial system computers to cease operation."* European Space Agency, Office of the Director General, "Inquiry Board Report: Ariane 5 Flight 501 Failure," Paris, France, July 19, 1996.

[2] "*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).... 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."* European Space Agency, Office of the Director General, "Inquiry Board Report: Ariane 5 Flight 501 Failure," Paris, France, July 19, 1996.

[3] Nuseibeh B, "Ariane 5: Who Dunnit?", IEEE Software, Volume 14 Issue 3, May-June 1997

[5] Jézéquel J-M; Meyer B, "Design by contract: the lessons of Ariane", Computer, Volume: 30 Issue 1, Jan 1997, pp 129-130

[6] *"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."* European Space Agency, Office of the Director General, "Inquiry Board Report: Ariane 5 Flight 501 Failure," Paris, France, July 19, 1996.

[7] ESA Software Engineering Standards Issue 2 (ESA PSS-05-0 Issue 2, February 1991

[8] *"Using requirements specification languages can eliminate many of these problems, and these range in rigor from structured English to formal methods such as Z or VDM. Formal methods should be considered for the specification of safety-critical systems."* ESA Software Engineering Standards Issue 2 (ESA PSS-05-0 Issue 2, February 1991

ref [cnt]: Editorial on the Sextant/Arianespace relationship was published in AW&ST the week of August 6, 1996..

ref [QA]: *"Unit, integration, system and acceptance testing of executable software is essential to assure its quality. Test plans, test designs, test case, test procedures and test reports are described in the SVVP. These*

should be reviewed by SQA personnel. They should monitor the testing activities carried out by the development team, including test execution. Additionally, other tests may be proposed in the SQAP. These may be carried out by SQA personnel." ESA Software Engineering Standards Issue 2 (ESA PSS-05-0 Issue 2, February 1991

Bibliography:

[B1] Computer (IEEE), *Object-Oriented Department*, January of 1997 (vol. 30, no. 2, pages 129-130)

[B2] European Space Agency, Office of the Director General, *"Inquiry Board Report: Ariane 5 Flight 501 Failure,"* Paris, France, July 19, 1996.

[B3] Le Lann G, *"An Analysis of the Ariane 5 Flight 501 Failure – A System Engineering Perspective"*, 10th IEEE Intl. ECBS Conference, March 1997,

[B4] Lowry M, *"Software Construction and Analysis Tools for Future Space Missions"*,TACAS 2002, LNCS 2280, pp 1-19, pub. Springer-Verlag Berlin Heidelberg 2002

[B5] Carlo Mazza et al. (Eds.), *(ESA) Software Engineering Standards*, entice Hall, 1994, ISBN 0-13-106568-8

Web bibliography: (All URLs were last reviewed on 24-04-2003)

[W1] http://esapub.esrin.esa.it/bulletin/bullet89/dalma89.htm

[W2] http://www.cs.mdx.ac.uk/research/SFC/Papers/AJMD_EuroMicro00.pdf

[W3] http://www.geocities.com/idmssql/idms93.htm

[W4] http://www.fmf.uni-lj.si/~jaklicg/arianne.htm

[W5] http://www.ability.org.uk/launch_vehicles.html

[W6] http://www.sohar.com/training/pdf/VV%20TRaining.pdf

[W7] http://www.damek.kth.se/RTC/SC3S/

[W8] http://home.att.net/~SpaceWeb/SPSM6000/ExpandedRefs.htm

[W9] http://flint.cs.yale.edu/shao/cs430/lectureNotes/lecture1.pdf

[W10] http://www.reference.com/Dir/Science/Technology/Space/Launch_Vehicles/

[W11] http://www.panelsoft.com/murphyslaw/sep01.htm

[W12] http://www.rcost.unisannio.it/antoniol/stat-mat/intro-4.pdf

[W13] http://www.mcs.le.ac.uk/admissions/postgraduate/PGOpps/node4.html

[W14] http://www.asq.org/pub/sqp/past/vol2_issue2/frm_ed.html

[W15] http://216.239.39.100/search?q=cache:VOwC9Vzh02UC:suif.stanford.edu/papers/Diduce.ps.gz+%22ARIANNE+5%22+%2BFailure&hl=en&ie=UTF-8

[W16] http://www.radio-list.com/Directory/Science/Technology/Space/LaunchVehicles/

[W17] http://www2.vuw.ac.nz/staff/stephen_marshall/SE/Failures/SE_Ariane.html

[W18] http://www.esa.int/export/esaLA/index.html

[W19] http://www.esa.int/export/esaLA/ASEVLU0TCNC_index_0.html

[W20] http://www.arianespace.com/site/images/ARIANE5_tech_GB.pdf

[W21] http://www.arianespace.com/site/index2.html

[W22] http://www.arianespace.com/site/launchstatus/status_sub_index.html

[W23] http://www.arianespace.com/site/images/ASAP5-manual.pdf

[W24] http://www.esa.int/export/esaLA/Pr_33_1996_p_EN.html

[W25] http://www.astronautix.com/lvs/ariane5.htm

[W26] http://java.sun.com/people/jag/Ariane5.html

[W27] http://www.siam.org/siamnews/general/ariane.htm

[W28] http://www.cafm.sbu.ac.uk/cs/people/jpb/teaching/ethics.html

[W29] http://www2.vuw.ac.nz/staff/stephen_marshall/SE/Failures/SE_Ariane.html

[W30] http://216.239.57.100/search?q=cache:UXXBFC7FN1cC:www.cigital.com/papers/download/crystal.ps+ariane+5+failure%2Blegal+consequences&hl=en&ie=UTF-8

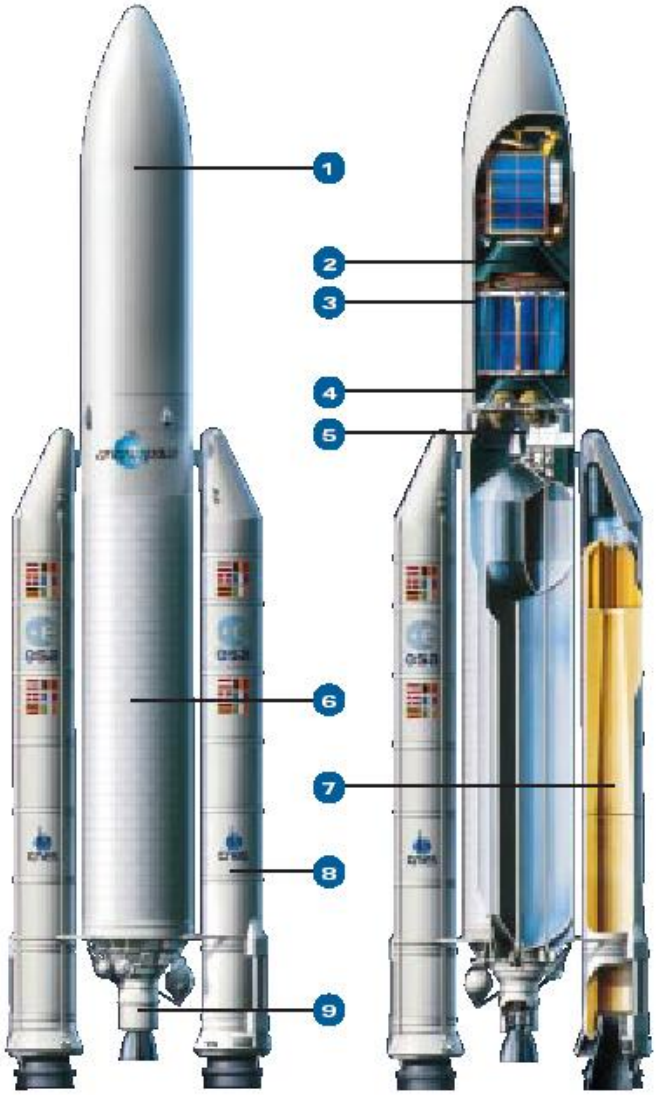
[W31] http://www.fei.br/eletrica/rbianchi/engesoft/suporte/ariane5-softeng.htm

[W32] http://archive.eiffel.com/doc/manuals/technology/contract/ariane/page.html

*The URLs of the web bibliography are links to the **specific web pages** used for reading material (research) around the subject.*

Appendix 1

In the following picture we can see the subcontractor employed in the creation of the Ariane 5 rocket divided by the section they constructed.



1. Payload fairing
Prime: Contraves Space
Subcontractors:
Aerospatiale Matra Lanceurs, DaimlerChrysler Aerospace, Dassault, SF Emmen, Framatome, Raufoss

2. Payload adapters
Prime: CASA, Matra Marconi Space, Saab Ericsson Space
Subcontractors:
Aerospatiale Matra Lanceurs, Dornier Satellitensisteme, Matra Marconi Space UK, Saab Ericsson Space

3. Speltra and Sylda 5
Prime: DaimlerChrysler Aerospace Dornier
Subcontractors:
Aerospatiale Matra Lanceurs, Dassault, Framatome, HRE, Raufoss

4. Vehicle equipment bay
Prime: Matra Marconi Space
Subcontractors: Alcatel Denmark Space, Alcatel ETCA, CASA, Crisa, DaimlerChrysler Aerospace, Dassault, Framatome, In-Snec, Raufoss, Saab Ericsson Space, Sextant,Thomson Hybrides

5. Storable propellant upper stage
Prime: DaimlerChrysler Aerospace
Subcontractors: Aerospatiale Matra Lanceurs, Alcatel Denmark, Space,Aljo,CASA, Dassault, Franke, Industria, Moog, Rellumix, Raufoss, Walther,Witzemann

6. Main cryogenic stage
Prime: Aerospatiale Matra Lanceurs
Subcontractors: Alcatel ETCA,Alcatel Denmark Space, Cryospace, DaimlerChrysler Aerospace, Elecma, Fokker Space, In-Snec, MAN Technologie, Sabca, Saft, SAT

7. Solid rocket motor
Prime: Europropulsion
Subcontractors: Andritz, FiatAvio, MAN Technologie, Regulus, Snecma

8. Solid rocket boosters
Prime: Aerospatiale Matra Lanceurs
Subcontractors: Fokker Space, Kongsberg, Raufoss, Sabca

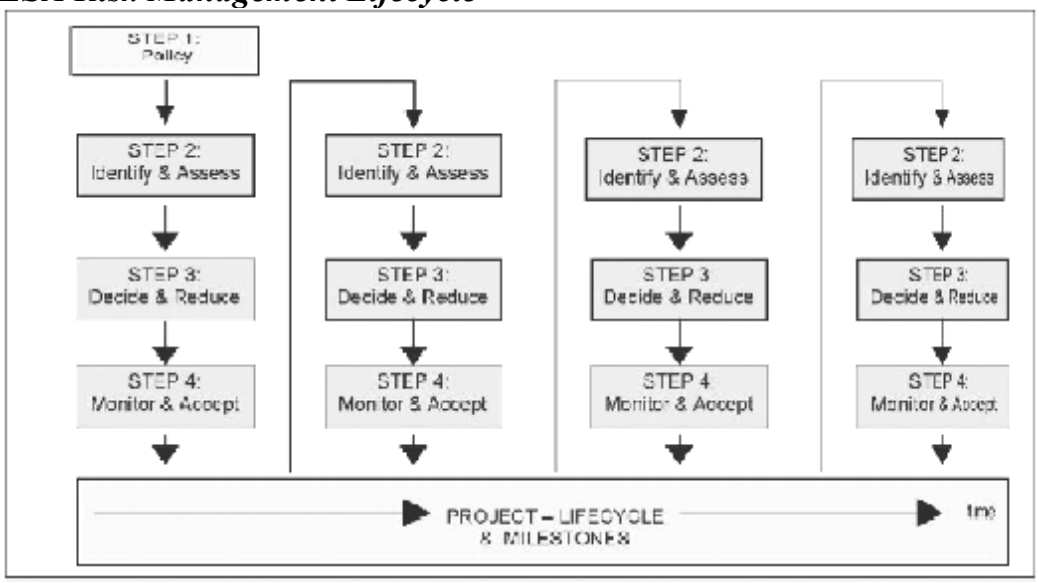
9. Vulcain propulsion system
Prime: Snecma
Subcontractors: Auxitrol, Avica, CASA, DaimlerChrysler, Aerospace, Devtec, Fagor, FiatAvio, MAN Technologie, MCG, Microtecnica, SNR, Stork,Techspace Aero,Vibrometer,Volvo Aero

Reference: [W20]

Appendix 2

Source: ESA publication (http://www.esa.int)

ESA Risk Management Lifecycle



Consequence Severity Categories

Consequence Severity of Risk Scenario	Severity Score	Impact on Performance	Impact on Schedule	Impact on Cost
	5	**Maximum:** Unacceptable, no alternatives exist	**Maximum:** Can't achieve major project milestone	**Maximum:** Cost increase > 15%
	4	**High:** Major reduction, but workarounds available	**High:** Project milestone slip ≥ 1 month, or project critical path impacted	**High:** Cost increase > 10%
	3	**Medium:** Moderate reduction, but workarounds available	**Medium:** Project team milestone slip ≤ 1 month	**Medium:** Cost increase > 5%
	2	**Low:** Moderate reduction, Some approach Retained	**Low:** Additional activities required, able To meet need dates	**Low:** Cost increase < 5%
	1	**Minimum:** Minimal or no impact	**Minimum:** Minimal or No impact	**Minimum:** Minimal or no impact