# INFORME DE LA AGENCIA ESPACIAL EUROPEA DEL ACCIDENTE DEL VUELO 501 DE ARIANE-5

---

París, 19 de Julio de 1996

**ARIANE-5**

**Fracaso del vuelo 501**

Informe de la Comisión de Investigación

Prof. J. L. LIONS

# INTRODUCCIÓN

El 4 de Junio de 1996, el vuelo inaugural de la lanzadera Ariane-5 resultó fallido. Tan sólo 40 segundos aproximadamente después de la iniciación de la secuencia de vuelo, a una altitud de aproximadamente 3700 m, la lanzadera se desvió de su ruta, se partió y explotó. Los ingenieros de los equipos del proyecto Ariane-5 de CNES & Industry empezaron inmediatamente a investigar el fallo. En los días siguientes, el Director General de la ESA y el Presidente de la CNES formaron una Comisión de Investigación independiente y nombraron a los siguientes miembros:

- Prof. Jacques-Louis Lions (Presidente), Academie des Sciences (Francia)
- Dr. Lennart Luebeck (Vicepresidente), Swedish Space Corporation (Suecia)
- D. Jean-Luc Fauquembergue, Delegation Generale pour l'Armement (Francia)
- D. Gilles Kahn, Institut National de Recherche en Informatique et en Automatique (INRIA), (Francia)
- Prof. Dr. Ing. Wolfgang Kubbat, Technical University of Darmstadt (Alemania)
- Dr. Ing. Stefan Levedag, Daimler Benz Aerospace (Alemania)
- Dr. Ing. Leonardo Mazzini, Alenia Spazio (Italia)
- D. Didier Merle, Thomson CSF (Francia)
- Dr. Colin O'Halloran, Defense Evaluation and Research Agency (DERA), (Reino Unido)

Las competencias asignadas a la Comisión requerían que la misma:

- determinara las causas del fallo en el lanzamiento,
- investigara si los tests de cualificación y de aceptación fueron apropiados en relación con el problema encontrado,
- recomendara acciones correctivas para eliminar las causas de las anomalías y otros posibles puntos débiles de los sistemas encontrados defectuosos.

La comisión comenzó su trabajo el 13 de Junio de 1996. Contó con la ayuda de un Comité Asesor Técnico compuesto por:

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

De acuerdo con estas competencias, la Comisión concentró sus investigaciones en las causas del fallo, los sistemas supuestamente responsables de ello, cualquier fallo de naturaleza similar en sistemas también similares, y acontecimientos que pudieran estar relacionados con el accidente. Consecuentemente, las recomendaciones hechas por la Comisión están limitadas a las áreas examinadas. El informe contiene el análisis del fallo, las conclusiones de la Comisión y sus recomendaciones en cuanto a medidas correctoras, la mayoría de las cuales deberían tomarse antes del próximo vuelo del Ariane-5. Además existe un informe de circulación restringida en el cual los resultados de las investigaciones de la Comisión están documentados técnicamente más en detalle. Aunque se consultaron los datos telemétricos almacenados durante el vuelo, la Comisión no ha emprendido la evaluación de estos datos. Tampoco ha llevado a cabo una revisión completa de la lanzadera entera y todos sus sistemas.

Este informe es el resultado de un esfuerzo colectivo de la Comisión, ayudada por los miembros del Comité Asesor Técnico.

Hemos (la Comisión) trabajado exhaustivamente para presentar una explicación muy precisa de las razones del fallo y para contribuir a la mejora del software del Ariane-5. Esta mejora es necesaria para asegurar el éxito del programa.

Los resultados de las investigaciones de la Comisión están basadas en presentaciones de los equipos del proyecto Ariane-5, y en documentación, lo que ha demostrado la alta calidad del programa Ariane-5 en lo que se refiere a trabajo de ingeniería en general y la integridad y disponibilidad de los documentos.

El Presidente de la Comisión.

# 1. EL FALLO

## 1.1 DESCRIPCIÓN GENERAL

Sobre la base de la documentación disponible y la información presentada a la Comisión, se ha observado lo siguiente:

La climatología en el lugar de lanzamiento en Kourou en la mañana del 4 de Junio de 1996 era aceptable para el lanzamiento, y no representó ningún problema para el desplazamiento de la lanzadera a la plataforma de lanzamiento. En particular, no había riesgo de relámpagos puesto que la fuerza del campo eléctrico medido en el lugar de lanzamiento era despreciable.

La cuenta atrás, que también comprende el llenado de la etapa principal, se llevó a cabo sin complicaciones hasta H0-7 minutos, cuando la lanzadera se puso en suspenso, pues los criterios de visibilidad no se cumplían al principio de la ventana de lanzamiento (08h35 hora local). Las condiciones de visibilidad mejoraron como se había previsto y el lanzamiento fue iniciado a H0=09h 33m 59s hora local (=12h 33m 59s Hora Universal). La ignición del motor Vulcain y los dos propulsores sólidos fue la nominal, así como el despegue. El vehículo realizó un vuelo nominal hasta aproximadamente H0+37 segundos. Poco después de ese momento, repentinamente se salió de rumbo, se partió y explotó. Una investigación preliminar de los datos de vuelo mostró:

- comportamiento nominal de la lanzadera hasta h=+36 segundos;
- fallo del Sistema de Referencia Inercial de reserva seguido inmediatamente por el fallo del Sistema de Referencia Inercial activo;
- Giro a la posición tope de las bocas de los dos propulsores sólidos y, poco después, del motor Vulcain, provocando un viraje brusco de la lanzadera;
- Autodestrucción de la lanzadera correctamente disparado por la ruptura de los enlaces entre los propulsores sólidos y la etapa principal.

El origen del fallo fue por tanto rápidamente localizado en el sistema de control de vuelo y más particularmente en los Sistemas de Referencia Inercial, que obviamente dejaron de funcionar casi simultáneamente sobre aproximadamente H0+36.7 segundos.

## 1.2 INFORMACIÓN DISPONIBLE

La información disponible sobre el lanzamiento incluye:

- datos telemétricos recibidos en tierra hasta H0+42 segundos
- datos de trayectoria de las estaciones de radar
- observaciones ópticas (cámaras de infrarrojos, películas) - inspección del material recuperado.

La totalidad de los datos telemétricos recibidos en Kourou fue transferida a la CNES/Toulouse donde dichos datos fueron convertidos en representaciones de los parámetros en función del tiempo. CNES suministró una copia de los datos a Aerospatiale, quien llevó a cabo análisis concentrándose principalmente en los datos concernientes al sistema eléctrico.

## 1.3 RECUPERACIÓN DE MATERIAL

La autodestrucción de la lanzadera ocurrió cerca de la plataforma de lanzamiento, a una altitud de aproximadamente 4000 m. Además, todos los fragmentos de la lanzadera cayeron al suelo, esparcidos en un área de aproximadamente 12 $Km^2$ al este de la plataforma de lanzamiento. Sin embargo, la recuperación del material fue difícil, pues este área está casi enteramente formada por manglares o sabanas.

A pesar de esto, fue posible recuperar de los fragmentos los dos Sistemas de Referencia Inercial. De particular interés fue aquel que funcionó en modo activo y dejó de funcionar el último, y para el cual, además, cierta información no estaba disponible en los datos telemétricos (la información transmitida a tierra no dejaba claro cuál de las dos

unidades había fallado primero). Los resultados del exámen de esta unidad fueron de gran ayuda para el análisis de la secuencia de fallos.

### 1.4 ANOMALÍAS NO RELACIONADAS OBSERVADAS

El análisis post-vuelo de la telemetría ha mostrado cierto número de anomalías que han sido remitidas a la Comisión. Son mayoritariamente de poca significación y de esperar en un vuelo de demostración.

Una anomalía que llamó particularmente la atención de la Comisión fue el desarrollo gradual, empezando en H0+22 segundos, de variaciones en la presión hidráulica de los actuadores de la boca del motor principal. Estas variaciones tenían una frecuencia de aproximadamente 10 Hz.

Hay algunas explicaciones preliminares como posibles causas de estas variaciones, las cuales están ahora bajo investigación.

Después de considerarlo, la Comisión ha formado la opinión de que esta anomalía, aunque significativa, no tiene ninguna relación con el fallo de Ariane 501.

## 2. ANÁLISIS DEL FALLO

### 2.1 CADENA DE ACONTECIMIENTOS TÉCNICOS

En términos generales, el Sistema de Control de Vuelo del Ariane-5 es de un diseño standard. La orientación de la lanzadera y sus movimientos en el espacio son medidos por un Sistema de Referencia Inercial (SRI). Éste tiene su propio computador interno, en el cual los ángulos y las velocidades se calculan sobre la base de la información de una plataforma inercial, con giroscopios láser y acelerómetros. Los datos del SRI se transmiten a través del bus de datos a la Computadora de a Bordo (OBC), la cual ejecuta el programa de vuelo y controla las bocas de los propulsores sólidos y el motor criogénico Vulcain, por medio de servoválvulas y actuadores hidráulicos.

Con el objetivo de mejorar la fiabilidad hay una redundancia considerable a nivel de equipos. Hay dos SRIs operando en paralelo, con idénticos hardware y software. Un SRI está activo y el otro está en stand-by, y si el OBC detecta que el SRI activo ha fallado inmediatamente conmuta al otro, siempre y cuando esta unidad funcione correctamente. Del mismo modo hay dos OBCs, y algunas otras unidades en el Sistema de Control de Vuelo están también duplicadas.

Basándose en la extensa documentación y datos del fallo del Ariane 501 puestos a disposición de la Comisión, se han establecido la siguiente cadena de acontecimientos, sus interrelaciones y sus causas, comenzando con la destrucción de la lanzadera y rastreando atrás en el tiempo hacia la causa primaria.

- La lanzadera se empezó a desintegrar hacia H0+39 segundos a causa de las altas cargas aerodinámicas debidas al ángulo de ataque de más de 20 grados que provocaron la separación de los propulsores de la etapa principal, disparando el mecanismo de autodestrucción de la lanzadera

- Este ángulo de ataque fue causado por deflexiones límite de las bocas de los propulsores sólidos y del motor principal Vulcain.
- Estas deflexiones de las bocas fueron ordenadas por el software del OBC sobre la base de los datos transmitidos por el Sistema de Referencia Inercial activo (SRI 2). Parte de estos datos en ese momento no contenían datos de vuelo correctos, pero mostraban la plantilla de diagnóstico de la computadora del SRI 2, por lo cual fueron interpretados como datos de vuelo.
- La razón por la que el SRI 2 no enviaba datos de orientación correctos fue que la unidad declaró una fallo debido a una excepción de software
- El OBC no pudo conmutar al SRI de reserva, el SRI 1 porque dicha unidad ya había dejado de funcionar durante el ciclo de datos previo (periodo de 72 milisegundos) por la misma razón que el SRI 2.
- La excepción de sofware interna del SRI fue causada durante la ejecución de una conversión de datos desde coma flotante a 64 bits hasta valor entero con signo de 16 bits. El número en coma flotante que fue convertido tenía un valor mayor del que podía ser representado por un entero con signo de 16 bits. Esto dio lugar a un Error de Operando. Las instrucciones de conversión de datos (en código Ada) no estaban protegidas de causar un Error de Operando, aunque otras conversiones de variables comparables en el mismo lugar en el código estaban protegidas.
- El error ocurrió en una parte del software que únicamente realiza alineamientos de la plataforma inercial. Este módulo software computa resultados significativos solamente antes del despegue. Tan pronto como la lanzadera despega, esta función deja de ser útil.
- La función de alineamiento está operativa durante 50 segundos después del comienzo del Modo de Vuelo de los SRIs, lo cual ocurre en H0-3 segundos para Ariane-5. Consecuentemente, cuando el despegue tiene lugar, la función continúa durante aproximadamente 40 segundos de vuelo. Esta secuencia de tiempo está basada en un requerimiento de Ariane-4 y no se requiere para Ariane-5.
- El Error de Operando ocurrió debido a un valor inesperadamente alto de un resultado de una función de alineamiento interno llamado BH, Horizontal Bias, relacionado con la velocidad horizontal detectada por la plataforma. Este valor es calculado como un indicador para la precisión de alineamiento con el tiempo.
- El valor de BH era mucho más alto que el esperado porque la primera parte de la trayectoria de Ariane-5 difiere de la misma en el Ariane-4 y los resultados en valores considerablemente altos de velocidad horizontal.

Los acontecimientos internos del SRI que llevaron al fallo han sido reproducidos por cálculos de simulación. Además, ambos SRIs fueron recuperados durante la investigación de la Comisión y el contexto del fallo fue precisamente determinado a partir de las lecturas de las memorias. En adición, la Comisión ha examinado el código del software el cual demostró ser consistente con el escenario del fallo. Los resultados de estos exámenes están documentados en el Informe Técnico.

Además, se establece más allá de la duda razonable que la cadena de acontecimientos arriba expuesta refleja las causas técnicas del fallo de Ariane 501.

## 2.2 COMENTARIOS SOBRE EL ESCENARIO DEL FALLO

En el escenario del fallo, las causas técnicas primarias son el Error de Operando al convertir la variable BH, y la falta de protección de esta conversión, lo que causó la parada de la computadora del SRI.

Se ha informado a la Comisión de que no todas las conversiones fueron protegidas porque se había fijado para la computadora del SRI un objetivo de carga de trabajo máxima del 80%. Para determinar la vulnerabilidad del código no protegido, se realizó un análisis sobre toda operación que pudiese dar lugar a una excepción, incluyendo un Error de Operando. En particular, la conversión de valores en coma flotante a enteros se analizó y las operaciones que incluían siete variables estaban en riesgo de dar lugar un Error de Operando. Esto dió lugar a que se añadiera protección a cuatro de las variables, de lo cual hay evidencia en el código Ada. Sin embargo, tres de las variables se dejaron desprotegidas. En el código fuente no se encontró directamente ninguna referencia se justificación. Dada la gran cantidad de documentación asociada con cualquier aplicación industrial, el asunto se obscureció, aunque no deliberadamente, de cualquier revisión externa.

La razón para que esas tres variables restantes, incluyendo la que denotaba la velocidad horizontal, estuvieran desprotegidas fue que o bien estaban físicamente limitadas o bien estaban en un gran margen de seguridad, un razonamiento que en el caso de la variable BH se demostró erróneo. Es importante hacer notar que la decisión de proteger ciertas variables pero no otras fue tomada consensuadamente entre los socios del proyecto a varios niveles contractuales

No hay evidencia de que ningún dato de trayectoria haya sido usado para analizar el comportamiento de las variables no protegidas, y es aún más importante hacer notar que fue consensuado el no incluir los datos de trayectoria de Ariane-5 en los requerimientos del SRI y las especificaciones.

Aunque la fuente del Error de Operando ha sido identificada, esto en sí mismo no causó el fallo de la misión. La especificación del mecanismo de manejo de excepciones también contribuyó al fallo. En el caso de cualquier clase de excepción, la especificación del sistema indicaba que: el fallo debía ser indicado en el bus de datos, el contexto del fallo debería ser almacenado en una memoria EEPROM (que fue recuperada y leída en Araine 501), y finalmente, el procesador del SRI debería ser apagado.

Fue la decisión de apagar el procesador la que finalmente resultó fatal. El reinicio no es factible debido a que la orientación es demasiado difícil de recalcular tras un apagado de procesador; además el Sistema de Referencia Inercial se convierte en inútil. La razón para esta acción drástica reside en la norma dentro del programa Ariane de direccionar solamente fallos hardware aleatorios. Desde este punto de vista los mecanismos de manejo de excepciones - o errores - están diseñados para un fallo hardware aleatorio que pueda ser manejado racionalmente por un sistema de recuperación.

Aunque el fallo fue debido a un error en el sistema de diseño de software, se pueden introducir mecanismos para mitigar este tipo de problemas. Por ejemplo las computadoras dentro de los SRIs podrían haber continuado con una provisión de sus

mejores estimaciones de la información de orientación requerida. Hay razones para ocuparse de que una excepción software pudiera ser permitida, o incluso requerida, para causar que un procesador parase durante el manejo de equipos críticos para la misión. De hecho, la pérdida de una función software correcta es grave porque el mismo software se ejecuta en las dos unidades SRI. En el caso de Ariane 501, esto resultó en la desconexión de dos unidades de equipamiento que aún eran críticas.

Los requerimientos originales que se tienen en cuenta para la operación continuada del software de alineamiento después del despegue fueron llevados a cabo después de hace más de 10 años para los modelos tempranos de Ariane, con el objetivo de manejar el improbable suceso de una suspensión de la cuenta atrás, entre -9 segundos, cuando el modo de vuelo empieza en el SRI de Ariane 4, y -5 segundos, cuando ciertos sucesos son iniciados en la lanzadera, los cuales llevan varias horas de reinicialización. El periodo seleccionado para esta operación de alineamiento continuada, 50 segundos después del comienzo del modo de vuelo, estaba basado en el tiempo necesario para que en equipo de tierra retomara el pleno control de la lanzadera en el caso de suspensión.

Esta especial prestación hacía posible con las versiones anteriores de Ariane el recomenzar la cuenta atrás sin esperar al alineamiento normal, lo cual lleva 45 minutos o más, por lo que la corta ventana de lanzamiento podía aún ser usada. De hecho, esta prestación fue usada una vez, en 1989 en el vuelo 33.

El mismo requisito no se aplica a Ariane-5, el cual tiene una secuencia de preparación diferente y fue mantenido por razones de uniformidad, presumiblemente basadas en la hipótesis de que, a menos de que se probara su necesidad, no era preciso hacer cambios en el software que funcionaba bien en Ariane-4.

Incluso en aquellos casos en los que el requisito es aún válido, es cuestionable que la función de alineamiento aún opere después de que la lanzadera haya despegado. El alineamiento de las plataformas mecánica y láser incluye complejas funciones de filtros matemáticos para alinear correctamente el eje x con el eje de gravedad y para encontrar la dirección norte a partir de los sensores de rotación de la Tierra. La asunción del alineamiento pre-vuelo es que la lanzadera se coloca en una posición fija y conocida. Además, la función de alineamiento se rompe totalmente cuando se realiza durante el vuelo, porque los movimientos medidos de la lanzadera se interpretan como desplazamientos de los sensores y otros coeficientes que caracterizan el comportamiento del sensor.

Retornando al error software, la Comisión desea puntualizar que el software es expresión de un diseño altamente detallado y no falla en el mismo sentido que un sistema mecánico. Además el software es flexible y expresivo, por lo tanto pide una alta demanda de requisitos, lo cual se convierte en implementaciones complejas que son difíciles de asesorar.

Un tema pendiente en el desarrollo del Ariane-5 es la corriente hacia la mitigación de los fallos aleatorios. El suministrados del SRI seguía únicamente las especificaciones dadas, las cuales estipulaban que en caso de que cualquier excepción fuese detectada el procesador debía ser detenido. La excepción que ocurrió no fue debida a un fallo aleatorio sino a un error de diseño. La excepción fue detectada, pero se manejó inapropiadamente porque la bajo la visión del software se debió considerar correcta

hasta que se demostrara lo contrario. La Comisión tiene razones para creer que esta visión se acepta también en otras áreas del diseño del software de Ariane-5. La Comisión está a favor de la visión contraria, el software debió ser asumido como erróneo hasta que la aplicación de los mejores métodos prácticos actuales demostraran que es correcto.

Esto significa que el software crítico - en el sentido de que el fallo de dicho software pone en peligro la misión - debería ser identificado a un nivel muy detallado, ese comportamiento excepcional debe ser aislado, y una política razonable de recuperación debe tener en cuenta fallos software.

## 2.3 LOS PROCEDIMIENTOS DE PRUEBA Y CUALIFICACIÓN

La cualificación del Sistema de Control de Vuelo para Ariane-5 sigue un procedimiento estandar que se realiza a los siguientes niveles:

- Cualificación de equipos
- Cualificación de software (software del Computador de a Bordo)
- Integración de etapa
- Pruebas de validación del Sistema.

La lógica aplicada es probar a cada nivel lo que no se pudo conseguir en el nivel previo, por lo tanto se provee una cobertura completa de las pruebas de cada subsistema y del sistema integrado.

Las pruebas a nivel de equipos fueron en el caso del SRI conducidas rigurosamente con respecto a todos los factores medioambientales y de hecho mas allá de lo que se esperaba para Ariane-5. Sin embargo, no se realizó ningún test para verificar que el SRI se comportaría correctamente cuando estuviera sujeto a las secuencias de cuenta atrás, de vuelo y de trayectoria de Ariane-5.

Es notable que por razones físicas, no es factible probar el SRI como "caja negra" en el medio ambiente de vuelo, a menos que uno haga una prueba de vuelo totalmente realista, pero es posible hacer pruebas en tierra inyectando señales acelerométricas simuladas de acuerdo con los parámetros de vuelo previstos, mientras se usa también una tabla de giros para simular los movimientos angulares de la lanzadera. Si se hubiese llevado a cabo una prueba así por parte del suministrador o como parte del test de aceptación, el mecanismo de fallo habría sido puesto de relieve.

La explicación principal para la ausencia de dicho test ya se ha mencionado anteriormente, pues la especificación del SRI (que se supone un documento de requisitos del SRI) no contiene los datos de trayectoria de Ariane-5 como requisito funcional.

La Comisión se ha percatado de que la especificación de los sistemas del SRI no indica las restricciones operacionales que surgen de la implementación elegida. Tal declaración de limitaciones, que debería ser obligatoria para cada dispositivo crítico para la misión, habría servido para identificar cualquier falta de cumplimiento con la trayectoria de Ariane-5.

La otra oportunidad principal de detectar el mecanismo de fallo de antemano fue durante los numerosos tests y simulaciones llevados a cabo en la Instalación de Simulación Funcional, ISF, que se encuentra en el emplazamiento del Arquitecto Industrial. El objetivo de los tests del ISF son cualificar:

- La realización de la guía, la navegación y el control en el paquete entero de vuelo,
- La operación de redundancia de sensores, - las funciones dedicadas de las etapas,
- El software de vuelo (Computador de a Bordo) y su cumplimiento con todos los equipos del Sistema Eléctrico de Control de Vuelo.

Se realizaron un gran número de simulaciones en bucle cerrado del vuelo completo simulando la operación del segmento de tierra, el flujo telemétrico y la dinámica de la lanzadera, con el objetivo de verificar:

- La trayectoria nominal
- Trayectorias degradadas con respecto a parámetros internos de la lanzadera
- Trayectorias degradadas con respecto a parámetros atmosféricos
- Fallos de equipos y el subsiguiente aislamiento del fallo y recuperación.

En estas pruebas muchos puntos del equipamiento estaban físicamente presentes y en ejercicio, pero no los dos SRIs, los cuales fueron simulados por módulos software específicamente diseñados. Algunos tests en bucle abierto, para verificar el cumplimiento con el OBC y el SRI, fueron realizados con el SRI real. Se entiende que fueron simples tests de integración eléctrica y tests de cumplimiento a "bajo nivel" (bus de comunicación).

No es obligatorio, aunque sí recomendable, que todas las partes del subsistema estén presentes en todos los tests a un nivel dado. A veces esto no es físicamente posible o no es posible probarlos completamente o de forma representativa. En estos casos es lógico reemplazarlos con simuladores pero solamente después de cerciorarse cuidadosamente de que los tests de niveles anteriores han cubierto todos los campos enteramente.

Este procedimiento es especialmente importante para el test final del sistema antes de que sea usado operacinalmente (los tests realizados en la lanzadera 501 no se mencionan porque no son específicos de la cualificación del Sistema Eléctrico de Control de Vuelo).

Con el objetivo de entender las explicaciones dadas sobre la decisión de no tener los dos SRIs en la simulación en bucle cerrado, es necesario describir las configuraciones de prueba que se podrían haber usado.

Como no es posible simular las grandes aceleraciones lineales de la lanzadera en los tres ejes sobre una plataforma de prueba (como se ha mencionado más arriba). hay dos maneras de colocar el SRI en el bucle:

- Ponerlo en una plataforma dinámica de tres ejes (para estimular los Giroscopios Láser en Anillo) y sustituir la salida analógica de los acelerómetros (que no pueden ser estimulados mecánicamente) mediante una simulación por medio de

un conector de entrada de prueba dedicado y una tabla electrónica diseñada para este propósito. Esto es similar al método mencionado en conexión con las pruebas posibles a nivel de equipamiento.
- Sustituir ambos, la salida analógica de los acelerómetros y los Giroscopios Lásre en Anillo por medio de un conector de entrada de prueba dedicado con señales producidas por la simulación.

La primera aproximación es parecida a proveer de una simulación precisa (dentro de los límites del ancho de banda de la tabla dinámica de tres ejes) y es bastante cara; la segunda es más barata y su rendimiento depende esencialmente de la precisión de la simulación. En ambos casos una gran parte de la electrónica y del software completo se prueba en el medio ambiente operacional real.

Cuando la filosofía del test del proyecto fue definida, la importancia de tener los SRIs en el bucle se tuvo en cuenta y se tomó la decisión de seleccionar el segundo método. En una etapa posterior del programa (en 1992), esta decisión se cambió. Se decidió no tener los SRIs reales en el bucle por las siguientes razones:

- Los SRIs debían considerarse plenamente cualificados a nivel de equipamiento
- La precisión del software de navegación en el OBC depende críticamente de la precisión en las medidas del SRI. En el ISF, esta precisión no se podía conseguir mediante aparatos electrónicos que crearan las señales de prueba.
- La simulación de los modos de error no es posible con equipos reales, sino solamente con modelos.
- El periodo base del SRI es de 1 milisegundo mientras que el de la simulación en el ISF es de 6 milisegundos. Esto se añade a la complejidad del interface electrónico y podía incluso reducir la precisión de la simulación.

La opinión de la Comisión es que estos argumentos eran válidos técnicamente, pero como el propósito de una prueba de simulación del sistema no es solamente verificar los interfaces sino también verificar el sistema como un todo para una aplicación particular, existía un riesgo al asumir que el equipo crítico tal como el SRI había sido validado por sí mismo, o por uso previo con Ariane-4.

Mientras que es deseable una alta precisión en la simulación, en los tests del sistema en el ISF es claramente mejor un compromiso en cuanto a precisión pero conseguir todos los demás objetivos, entre ellos probar la correcta integración en el sistema de equipos como el SRI. La precisión del sistema de guía puede ser efectivamente demostrada por análisis y simulación por ordenador.

Bajo esta cabecera se debería hacer notar finalmente que los consiguentes medios de prevenir fallos son las revisiones, las cuales son una parte integral del proceso de diseño y cualificación, a las cuales son llevadas a cabo a todos los niveles e incluyen a todos los socios mayoritarios del proyecto (así como socios externos). En un programa de este tamaño, literalmente miles de problemas y fallos potenciales son manejados con éxito en el proceso de revisión y obviamente no es fácil detectar errores de diseño de software del tipo del que fue la causa técnica principal del fallo de Ariane 501. De todas formas, es evidente que las limitaciones del software del SRI no fue analizado plenamente en las revisiones, y no se tuvo en cuenta que la cobertura del test era inadecuada al exponerse a tales limitaciones. Ni lo fueron las posibles implicaciones de permitir que el software

de alineamiento operara durante el vuelo. A estos respectos, el proceso de revisión fue un factor que contribuyó al fallo.

### 2.4 OTRAS POSIBLES DEBILIDADES DEL SISTEMA IMPLICADAS

De acuedo con sus competencias, la Comisión ha examinado otras posibles debilidades, principalmente en el Sistema de Control de Vuelo. No se encontraron debilidades relacionadas con el fallo, pero a pesar del corto tiempo disponible, la Comisión ha dirigido una extensa revisión del Sistema de Control de Vuelo basada en la experiencia ganada durante el análisis del fallo.

La revisión ha cubierto las siguientes áreas:

- El diseño del sistema eléctrico,
- Software implementado a bordo en susbsistemas además del Sistema de Referencia Inercial,
- El OBC y el software del programa de vuelo.

Además, la Comisión ha hecho un análisis de los métodos aplicados en el programa de desarrollo, en particular con respecto a la metodología de desarrollo del software.

Los resultados de estos esfuerzos se han documentado en el Informe Técnico y la Comisión espera que contribuirán a mejoras del Sistema de Control de Vuelo del Ariane-5 y su software.

## 3. CONCLUSIONES

### 3.1 RESULTADOS

La Comisión ha alcanzado las siguientes conclusiones:

- Durante la campaña de preparación del lanzamiento y la cuenta atrás no ocurrieron sucesos relacionados con el fallo
- Las condiciones meteorológicas a la hora del lanzamiento eran aceptables y no jugaron ningún papel en el fallo. Ningún otro factor externo de relevancia ha sido encontrado.
- La ignición del motor y el despegue fueron esencialmente nominales y los efectos medioambientales (ruido y vibración) de la lanzadera y la carga útil no se encontraron relevantes para el fallo. El rendimiento de la propulsión estaba dentro de especificaciones.
- 22 segundos después de H0 (comando de ignición del motor principal criogénico), empezaron a aparecer variaciones de frecuencia 10 Hz en la presión hidráulica de los actuadores que controlan la boca del motor principal. Este fenómeno es significativo y no ha sido explicado plenamente, pero después de considerarlo no ha sido encontrado relevante para el fallo.
- A los 36.7 segundos después de H0 (aproximadamente 30 segundos después del despegue) la computadora del sistema de referencia inercial de reserva, que trabajaba en stand-by para la guía y el control de orientación, perdió su operatividad. Esto fue causado por una variable interna relacionada con la

velocidad horizontal de la lanzadera, que excedió el límite existente en el software del computador.

- Aproximadamente 0.05 segundos después el sistema de referencia inercial activo, idéntico al de reserva en hardware y software, falló por la misma razón. Como el sistema inercial de reserva ya no era operativo, la información correcta de guía y orientación no se pudo obtener más y la pérdida de la misión fue inevitable.
- Como resultado de su fallo, el sistema de referencia inercial activo transmitió esencialmente información de diagnóstico a la computadora principal de la lanzadera, que fue interpretada como información de vuelo y usada para cálculos de control de vuelo.
- Sobre la base de estos cálculos la computadora principal ordenó a las bocas de los propulsores, y algo después a la boca del motor principal también, que hicieran una enorme corrección para una desviación de orientación que no había ocurrido.
- Ocurrió un rápido cambio de orientación lo cual causó que la lanzadera se desintegrara a los 39 segundos después de H0 debido a fuerzas aerodinámicas.
- La destrucción fue automáticamente iniciada sobre la desintegración, como estaba diseñado, a una altitud de 4 Km y una distancia de 1 Km de la plataforma de lanzamiento.
- Los fragmentos se esparcieron sobre un área de 5 x 2.5 $Km^2$. Entre el equipo recuperado estaban los dos sistemas de referencia inerciales. Han sido usados para el análisis.
- El análisis post-vuelo de los datos de telemetría han listado cierto número de anomalías adicionales que están siendo investigadas pero no han sido consideradas significativas para el fallo.
- El sistema de referencia inercial de Ariane-5 es esencialmente común a un sistema que actualmente está volando en Ariane-4. La parte de este software que causó la interrupción en los computadores del sistema inercial se usa antes del lanzamiento para alinear el sistema de referencia inercial y, en Ariane-4, también para habilitar un rápido realineamiento del sistema en caso de una suspensión tardía de la cuenta atrás. Esta función de realineamiento, que no sirve para nada en el Ariane-5, fue aún así retenida por razones de comunalidad y permitida, como en Ariane-4, su operación durante aproximadamente 40 segundos después del despegue.
- Durante el diseño del software del sistema de referencia inercial usado para Ariane-4 y Ariane-5, se tomó la decisión de que no era necesario proteger la computadora del sistema inercial de perder su operatividad por un valor excesivo de la variable relacionada con la velocidad horizontal, una protección de que habían sido provistas otras variables del software de alineamiento. Cuando se tomó esta decisión, no fueron analizados o plenamente comprendidos los valores que esta variable en particular podía asumir cuando el software de alineamiento operara tras el despegue.
- En los vuelos de Ariane-4 usando el mismo tipo de sistema de referencia inercial no ha habido tal fallo porque la trayectoria durante los primeros 40 segundos de vuelo es tal que la variable particular relacionada con la velocidad horizontal no puede alcanzar, con un adecuado margen operacional, un valor más allá del límite presente en el software.
- Ariane-5 tiene una aceleración inicial alta y una trayectoria que lleva a una elevación del valor de la velocidad horizontal que es cinco veces más rápida que

en Ariane-4. El valor más alto de velocidad horizontal generado para Ariane-5, dentro del marco de tiempo de 40 segundos, causó un valor excesivo que provocó que cesara la operación de los computadores del sistema inercial.

- El propósito del proceso de revisión, que incluye a todos los socios mayoritarios del programa Ariane-5, es validar decisiones de diseño y obtener cualificación de vuelo. En este proceso, las limitaciones del software de alineamiento no fueron plenamente analizadas y las posibles implicaciones de permitir su función durante en vuelo no se tuvieron en cuenta.
- La especificación del sistema de referencia inercial y los tests realizados a nivel de equipamiento no incluyeron específicamente los datos de trayectoria de Ariane-5. Consecuentemente la función de realineamiento no fue probada bajo condiciones de vuelo simuladas de Araine-5, y el error de diseño no fue descubierto.
- Hubiera sido técnicamente factible incluir casi el sistema de referencia inercial entero en las simulaciones globales que se realizaron. Por ciertas razones se decidió usar la salida simulada del sistema de referencia inercial, no el sistema propiamente dicho o su simulación detallada. Si el sistema hubiera sido incluido, el fallo se hubiese podido detectar.
- Las simulaciones post-vuelo se han llevado a cabo en un computador con software del sistema de referencia inercial y con un medio ambiente simulado, incluyendo los datos de la trayectoria real del vuelo Ariane 501. Estas simulaciones han reproducido fielmente la cadena de acontecimientos que llevaron al fallo de los sistemas de referencia inercial.

### 3.2 CAUSA DEL FALLO

El fallo de Ariane 501 fue causado por la completa pérdida de guía e información de orientación 37 segundos después del comienzo de la secuencia de ignición del motor principal (30 segundos después del despegue). Esta pérdida de información fue debida a errores de especificación y diseño en el software del sistema de referencia inercial.Las extensas revisiones y tests llevados a cabo durante el programa de desarrollo del Ariane-5 no incluyó el adecuado análisis y prueba del sistema de referencia inercial o del sistema de control de vuelo completo, lo cual podría haber detectado los fallos potenciales.

# 4. RECOMENDACIONES

Sobre la base de sus análisis y conclusiones, la Comisión hace las siguientes recomendaciones:

- Desconexión de la función de alineamiento del sistema de referencia inercial inmediatamente después del despegue. Más generalmente, ninguna función software debería ser ejecutada durante el vuelo salvo necesidad.
- Preparar una instalación de prueba que incluya tanto equipamiento real como sea factible técnicamente, inyectar datos de entrada reales, y realizar un test del sistema completo en bucle cerrado. Las simulaciones completas deben tener lugar antes de cualquier misión. Una gran cobertura de test debe ser obtenida.
- No permitir que ningún sensor, como el sistema de referencia inercial, pare de enviar datos lo mejor posibles.

- Organizar, para cada unidad de equipamiento que incorpore software, una revisión de cualificación de software específica. El Arquitecto Industrial deberá tomar parte en estas revisiones e informar del test del sistema completo realizado con el equipo. Todas las restricciones en el uso del equipamiento deberán estar explícitas para la Comisión de Revisión. Hacer todo el software crítico un Asunto Controlado de Configuración (CCI).
- Revisar todo el software de vuelo (incluyendo software implementado) y en particular:
    - Identificar todas las asunciones implícitas hechas por el código y sus documentos de justificación sobre los valores de cantidades provistas por el equipamiento. Probar estas asunciones contra las restricciones en el uso del equipamiento.
    - Verificar el rango de valores tomados por cualquier variable interna o de comunicación en el software.
    - Soluciones a problemas potenciales en el software del OBC, prestando particular atención sobre la conmutación de OBC, debería ser propuesta por el equipo del proyecto y revisada por un grupo de expertos externos, que deberán informar a la Comisión de Cualificación del OBC.
- Donde sea técnicamente factible, considerar el aislamiento de excepciones a tareas y proveer de capacidad de recuperación.
- Proveer de más datos a la telemetría sobre el fallo de cualquier componente, para que la recuperación del equipo sea menos esencial.
- Reconsiderar la definición de componentes críticos, tomando en cuenta fallos de origen software (particularmente fallos en puntos simples).
- Incluir participantes externos (al proyecto) cuando se revisen las especificaciones, código y documentos de justificación. Asegurarse de que estas revisiones consideran la esencia de los argumentos, además de probar que se han realizado las verificaciones.
- Incluir los datos de trayectoria en las especificaciones y los requisitos de las pruebas.
- Revisar la cobertura de las pruebas del equipamiento existente y extenderla hasta donde se estime necesario.
- Darle a los documentos de justificación las mismas atenciones que al código. Mejorar la técnica de mantenimiento de la consistencia del código y sus justificaciones.
- Crear un equipo que preparará el procedimiento para cualificar el software, propondrá reglas estrictas para confirmar dicha cualificación, y cerificará que especificación, verificación y test del software son de una alta y consistente calida en el programa Ariane-5. Se considerará la inclusión de expertos RAMS externos.
- Una organización más transparente de la cooperación entre los socios en el programa Ariane-5 debería ser considerada. La cooperación cercana en ingeniería, con autoridad y responsabilidad claramente delimitadas, es necesaria para conseguir la coherencia del sistema, con interfaces claros y simples entre socios.