

TEXTO 1

<http://www.around.com/ariane.html>

Copyright 1996 James Gleick

Publicado por primera vez en la revista New York Times el 1 de diciembre de 1996.

UN ERROR Y UN ACCIDENTE

A veces un error es más que una molestia



ariana 5

A la Agencia Espacial Europea le tomó 10 años y 7 mil millones de dólares producir Ariane 5, un cohete gigante capaz de poner en órbita un par de satélites de tres toneladas con cada lanzamiento y destinado a darle a Europa una supremacía abrumadora en el negocio espacial comercial.

Todo lo que se necesitó para hacer explotar ese cohete a menos de un minuto de su viaje inaugural en junio pasado, esparciendo escombros ardientes por los manglares de la Guayana Francesa, fue un pequeño programa de computadora que intentaba meter un número de 64 bits en un espacio de 16 bits.

Un error, un fallo. De todas las líneas de código descuidadas registradas en los anales de la informática, ésta puede ser la más devastadoramente eficiente. A partir de entrevistas con expertos en cohetes y un análisis elaborado para la agencia espacial, un camino claro del error aritmético a la destrucción total emerge.



Fragmentos del fallido lanzamiento del Ariane 501

Para reproducir la cinta al revés:

39 segundos después del lanzamiento, cuando el cohete alcanzó una altitud de dos millas y media, un mecanismo de autodestrucción acabó con el Ariane 5, junto con su carga útil de cuatro satélites científicos costosos y sin seguro. La autodestrucción se desencadenó automáticamente porque las fuerzas aerodinámicas arrancaban los propulsores del cohete.

Esta desintegración había comenzado un instante antes, cuando la nave espacial se desvió de su rumbo bajo la presión de las tres potentes toberas de sus propulsores y del motor principal. El cohete estaba realizando una brusca corrección de rumbo que no era necesaria, compensando un giro equivocado que no se había producido.

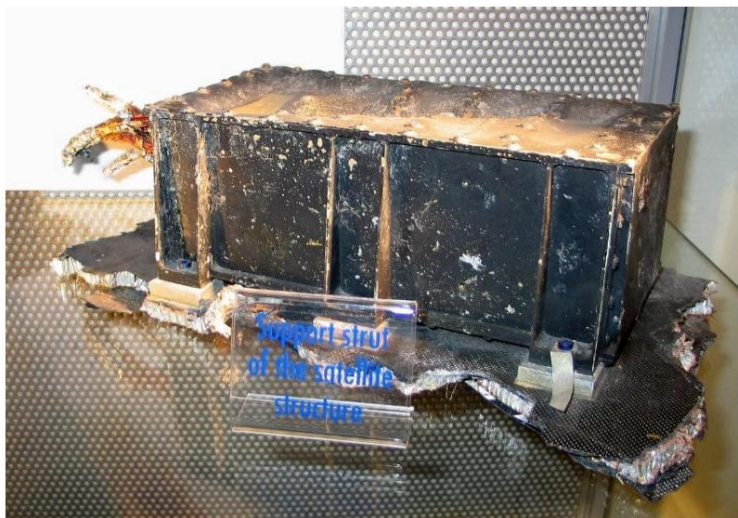
La dirección estaba controlada por la computadora de a bordo, que pensó erróneamente que el cohete necesitaba un cambio de rumbo debido a los números provenientes del sistema de guía inercial. Ese dispositivo utiliza giroscopios y acelerómetros para rastrear el movimiento. Los números parecían datos de vuelo (datos de vuelo extraños e imposibles) pero en realidad eran un mensaje de error de diagnóstico. De hecho, el sistema de guía se había apagado.

Este apagado se produjo 36,7 segundos después del lanzamiento, cuando la propia computadora del sistema de guía intentó convertir un dato (la velocidad lateral del cohete) de un formato de 64 bits a un formato de 16 bits. El número era demasiado grande y se produjo un error de desbordamiento. Cuando el sistema de guía se apagó, pasó el control a una unidad idéntica y redundante, que estaba allí para brindar respaldo en caso de que ocurriera tal falla. Pero la segunda unidad había fallado de la misma manera unos milisegundos antes. ¿Y por qué no? Estaba ejecutando el mismo software.

Este error pertenece a una especie que ha existido desde que los primeros programadores de computadoras se dieron cuenta de que podían almacenar números como secuencias de bits, átomos de datos, unos y ceros: 1001010001101001. . . Un error como este podría bloquear una hoja de cálculo o un procesador de textos en un mal día. Sin embargo, normalmente, cuando un programa convierte datos de un formulario a otro, las conversiones están protegidas por líneas adicionales de código que detectan errores y se recuperan sin problemas. De hecho, muchas de las conversiones de datos en la programación del sistema de orientación incluían dicha protección.

Pero en este caso, los programadores habían decidido que esta cifra de velocidad en particular nunca sería lo suficientemente grande como para causar problemas. Después de todo, nunca antes lo había sido. Desgraciadamente, el Ariane 5 era un cohete más rápido que el Ariane 4. Un absurdo adicional: el cálculo que contenía el error, que desactivó el sistema de guía, que confundió al ordenador de a bordo, que desvió el rumbo del cohete, en realidad no sirvió para nada una vez que el cohete estaba en el aire. Su única función era alinear el sistema antes del lanzamiento. Entonces debería haberse apagado. Pero los ingenieros decidieron hace mucho tiempo, en una versión anterior del Ariane, dejar esta función activa durante los primeros 40 segundos de vuelo, una "característica especial" destinada a facilitar el reinicio del sistema en caso de una breve pausa en el vuelo. La cuenta regresiva.

Los europeos esperan lanzar un nuevo Ariane 5 la próxima primavera, esta vez con un nuevo "arquitecto de software" que supervisará un proceso de simulación terrestre más intensiva y, esperan, realista. La simulación es la gran esperanza de los depuradores de software de todo el mundo, aunque nunca puede anticipar todas las características de la vida real. "Los detalles más pequeños pueden tener consecuencias terribles", afirma Jacques Durand, director del proyecto, en París. "Esto no es sorprendente, especialmente en un sistema de software complejo como este".



Puntal de soporte recuperado de la estructura satélite.

Hoy en día, tenemos sistemas de software complejos en todas partes. Los tenemos en nuestros lavavajillas y en nuestros relojes de pulsera, aunque no son tan críticos. Tenemos computadoras en nuestros automóviles: de 15 a 50 microprocesadores, dependiendo de cómo se cuenten: en el motor, la transmisión, las suspensiones, la dirección, los frenos y todos los demás subsistemas importantes. Cada uno ejecuta su propio software, sin duda probado, simulado y depurado minuciosamente.

Bill Powers, vicepresidente de investigación de Ford, dice que la potencia informática de los automóviles se dedica cada vez más no sólo al control real sino también al diagnóstico y la planificación de contingencias: "¿Debería abortar la misión, y si la aborto, adónde iría?" él dice. "También tenemos lo que se llama una estrategia de emergencia". Es decir, en el peor de los casos, se supone que el automóvil se comporta más o menos normalmente, como un automóvil de la era anterior a las computadoras, en lugar de, digamos, encargarse de desviarse hacia el árbol más cercano.

Los investigadores europeos optaron por no señalar como culpable a ningún contratista o departamento en particular. "Se tomó una decisión", escribieron. "No fue analizado ni comprendido completamente". Y "no se dieron cuenta de las posibles implicaciones de permitirle continuar funcionando durante el vuelo". No intentaron calcular cuánto tiempo o dinero se ahorró al omitir el código de protección contra errores estándar.

"La junta desea señalar", añadieron, con la magnífica insipidez de muchos informes oficiales de accidentes, "que el software es la expresión de un diseño muy detallado y no falla en el mismo sentido que un sistema mecánico". No. Falla en un sentido diferente. El software creado a lo largo de años a partir de millones de líneas de código, ramificándose, desplegándose y entrelazándose, llega a comportarse más como un organismo que como una máquina.

"Hoy en día no hay vida sin software", afirma Frank Lanza, vicepresidente ejecutivo del fabricante de cohetes estadounidense Lockheed Martin. "El mundo probablemente simplemente colapsaría". Afortunadamente, señala, el software realmente importante tiene una fiabilidad del 99,9999999 por ciento. Al menos, hasta que no sea así.

TEXTO 2

ERROR MÉTRICO CAUSÓ LA PÉRDIDA DEL ORBITER DE LA NASA

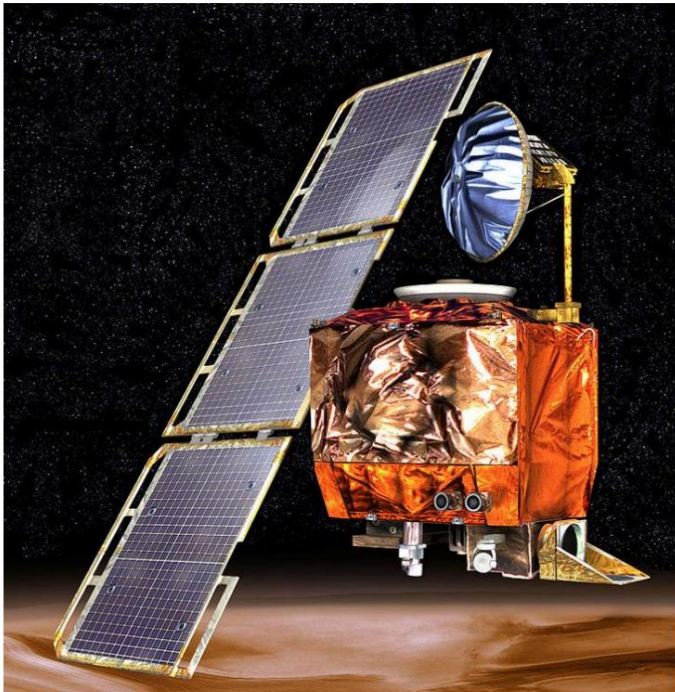
El Climate Orbiter de la NASA se perdió el 23 de septiembre de 1999

30 de septiembre de 1999

Web publicado a las: 4:21 pm EDT (2021 GMT)

Por Robin Lloyd

Redactor senior interactivo de CNN



Mars Observer en la instalación de mantenimiento de cargas peligrosas

(CNN) -- La NASA perdió un orbitador de Marte de 125 millones de dólares porque un equipo de ingeniería de Lockheed Martin usó unidades de medida inglesas, mientras que el equipo de la agencia usó el sistema métrico más convencional para una operación clave de la nave espacial, según un hallazgo de revisión publicado el jueves.

El desajuste de las unidades impidió que la información de navegación se transfiriera entre el equipo de la nave espacial Mars Climate Orbiter en Lockheed Martin en Denver y el equipo de vuelo en el Jet Propulsion Laboratory de la NASA en Pasadena, California.

Lockheed Martin ayudó a construir, desarrollar y operar la nave espacial para la NASA. Sus ingenieros proporcionaron comandos de navegación para los propulsores del Climate Orbiter en unidades inglesas, aunque la NASA ha estado utilizando predominantemente el sistema métrico desde al menos 1990.

Nadie está señalando a Lockheed Martin, dijo Tom Gavin, el administrador del JPL a quien reportan todos los gerentes de proyectos.

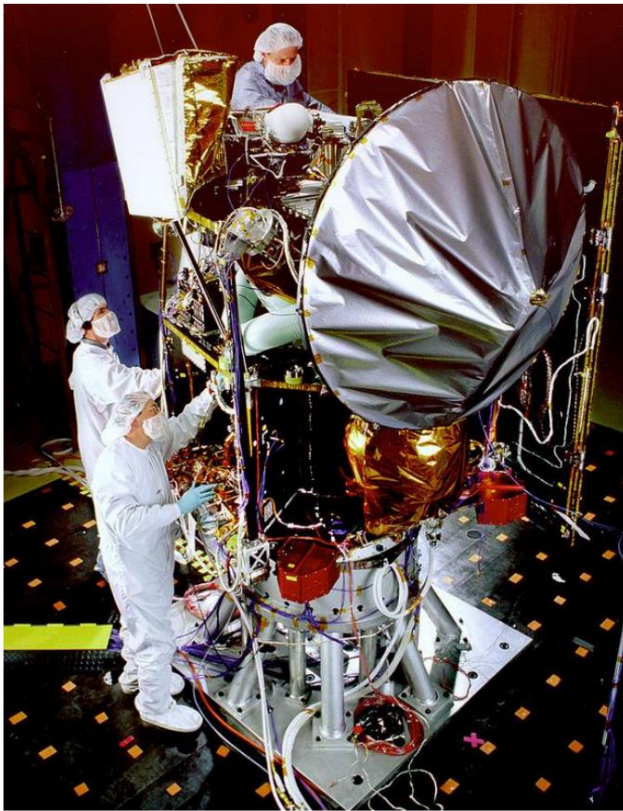
"Este es un problema de proceso de extremo a extremo", dijo. "Un solo error como este no debería haber causado la pérdida de Climate Orbiter. Algo salió mal en los procesos de nuestro sistema en los controles y equilibrios que tenemos y debería haber detectado esto y solucionarlo".

El hallazgo provino de un panel de revisión interna del JPL que informó la causa a Gavin el miércoles. El grupo incluía unos 10 especialistas en navegación, muchos de los cuales se retiraron recientemente del JPL.

"Han estado analizando esto desde el viernes por la mañana después de la pérdida", dijo Gavin.

El accidente de navegación acabó con la misión en un día en el que los ingenieros esperaban celebrar la entrada de la nave en la órbita de Marte.

Después de un viaje de 286 días, la sonda encendió su motor el 23 de septiembre para ponerse en órbita.



Mars Climate Orbiter sometido a pruebas acústicas.

El motor se encendió, pero la nave espacial se acercó a 60 kilómetros (36 millas) del planeta, unos 100 kilómetros más cerca de lo previsto y unos 25 kilómetros (15 millas) por debajo del nivel en el que podría funcionar correctamente, dijeron los miembros de la misión.

Los últimos hallazgos muestran que el sistema de propulsión de la nave espacial se sobrecalentó y quedó inutilizado cuando el Climate Orbiter se sumergió profundamente en la atmósfera, dijo el portavoz del JPL, Frank O'Donnell.

Eso probablemente impidió que el motor completara su funcionamiento, por lo que Climate Orbiter probablemente atravesó la atmósfera, continuó más allá de Marte y ahora podría estar orbitando el sol, dijo.

Climate Orbiter debía transmitir datos de una próxima misión asociada llamada Mars Polar Lander, programada para aterrizar en Marte en diciembre. Ahora los planificadores de la misión están trabajando en cómo transmitir sus datos a través de su propia radio y de otro orbitador que ahora orbita el planeta rojo.

Climate Orbiter y Polar Lander fueron diseñados para ayudar a los científicos a comprender la historia del agua en Marte y el potencial de vida en el pasado del planeta. Hay pruebas contundentes de que Marte alguna vez estuvo inundado de agua, pero los científicos no tienen respuestas claras sobre dónde fue el agua y qué la ahuyentó.

La NASA ha convocado dos paneles para investigar lo que llevó a la pérdida del orbitador, incluido el panel interno de revisión por pares que publicó el hallazgo del jueves. La NASA también planea formar una tercera junta (un panel de revisión independiente) para investigar el accidente.

Sistema métrico utilizado por la NASA durante muchos años.

Hace varios años, cuando se estaba desarrollando la misión Cassini a Saturno, apareció un documento de la NASA que establecía el sistema métrico para todas las unidades de medida, dijo Gavin.

El sistema métrico se utiliza para la misión Polar Lander, así como para las próximas misiones a Marte, dijo.

Los hallazgos de ese panel de revisión ahora están siendo estudiados por un segundo grupo: una junta de revisión especial encabezada por John Casani, que buscará los procesos que no lograron encontrar la métrica de la discrepancia en inglés. Casani se retiró del JPL hace dos meses como ingeniero jefe del laboratorio.

"Vamos a ver cómo se transfirieron los datos", dijo Gavin. "¿Cómo entró originalmente en el sistema en unidades inglesas? ¿Cómo se transfirió? Cuando estábamos haciendo comprobaciones de navegación y Doppler (distancia y velocidad), ¿por qué no lo encontramos?"

"La gente comete errores", dijo Gavin. "El problema aquí no fue el error. Fue nuestra incapacidad de mirarlo de principio a fin y encontrarlo. Es injusto confiar en una sola persona".

Lockheed Martin, que no respondió de inmediato a una llamada telefónica para solicitar comentarios, está construyendo orbitadores y módulos de aterrizaje para futuras misiones a Marte, incluida una que se lanzará en 2001 y una misión que devolverá algunas rocas de Marte a la Tierra dentro de unos años.

También ha ayudado con la misión Polar Lander, que aterrizará en Marte el 3 de diciembre y realizará una misión de 90 días para estudiar el clima marciano. También está diseñado para extender un brazo robótico que excavará en el suelo marciano cercano y buscará señales de agua.

Los administradores de la NASA han dicho que la misión Polar Lander continuará según lo planeado y arrojará respuestas a las mismas preguntas científicas originalmente planeadas, aunque el módulo de aterrizaje tendrá que transmitir sus datos a la Tierra sin la ayuda de Climate Orbiter.

Causa de la falla

El 10 de noviembre de 1999, la Junta de Investigación de Accidentes del Mars Climate Orbiter publicó un informe de la Fase I, que detalla los problemas sospechosos encontrados con la pérdida de la nave espacial. Anteriormente, el 8 de septiembre de 1999, se calculó la Maniobra de Corrección de Trayectoria-4 y luego se ejecutó el 15 de septiembre de 1999. Su objetivo era colocar la nave espacial en una posición óptima para una maniobra de inserción orbital que llevaría la nave espacial alrededor de Marte a una altitud de 226 kilómetros el 23 de septiembre de 1999. Sin embargo, durante la semana entre el TCM-4 y la maniobra de inserción orbital, el equipo de navegación indicó que la altitud puede ser mucho menor de lo previsto, entre 150 y 170 kilómetros. Veinticuatro horas antes de la inserción orbital, los cálculos situaban al orbitador a una altitud de 110 kilómetros; 80 kilómetros es la altitud mínima que se pensaba que Mars Climate Orbiter era capaz de sobrevivir durante esta maniobra. Los cálculos posteriores al fallo mostraron que la nave espacial estaba en una trayectoria que habría llevado al orbitador a 57 kilómetros de la superficie, donde la nave probablemente se desintegró debido a las tensiones atmosféricas.

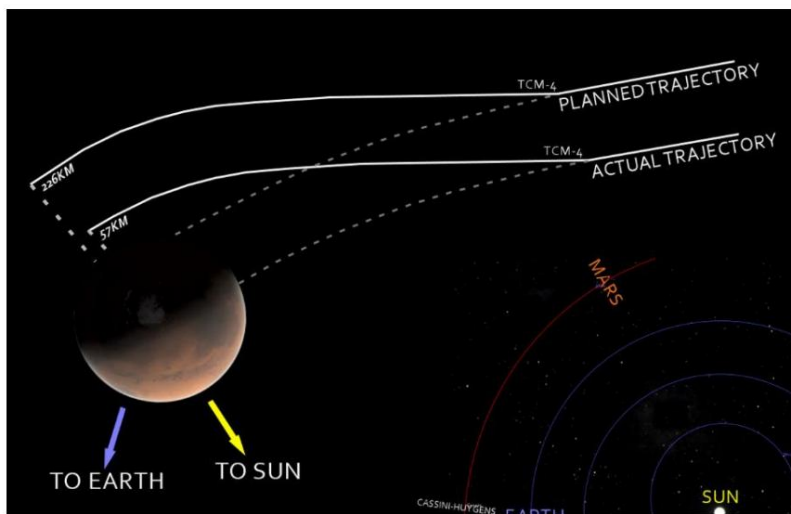


Diagrama que compara las trayectorias previstas y reales del Orbitador.

La causa principal de esta discrepancia fue que una pieza de software terrestre suministrada por Lockheed Martin produjo resultados en una unidad habitual de los Estados Unidos ("American"), contrariamente a su Especificación de Interfaz de Software (SIS), mientras que un segundo sistema, suministrado por la NASA, que utilizaron esos resultados esperaban que estuvieran en unidades métricas, de acuerdo con el SIS. El software que calculó el impulso total producido por el encendido de los propulsores calculó los resultados en libras-segundo. El cálculo de la trayectoria utilizó estos resultados para corregir la posición prevista de la nave espacial por los efectos del encendido de los propulsores. Este software esperaba que sus entradas estuvieran en newton-segundos.

La discrepancia entre la posición calculada y medida, lo que resulta en una discrepancia entre la altitud de inserción orbital deseada y real, había sido notada anteriormente por al menos dos navegantes, cuyas preocupaciones fueron descartadas. Se convocó una reunión de ingenieros de software de trayectoria, operadores de software de trayectoria (navegadores), ingenieros de propulsión y gerentes para considerar la posibilidad de ejecutar la Maniobra de Corrección de Trayectoria-5, que estaba en el cronograma. Los asistentes a la reunión recuerdan un acuerdo para realizar TCM-5, pero finalmente no se hizo.