Derechos de autor 1996 James Gleick

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

Un error y un choque.

**A veces un bug es más que un simple error.**

A la Agencia Espacial Europea le tomó 10 años y $7 billones para producir Ariane 5, un cohete gigante capaz de lanzar fuera de órbita a un par de satélites de tres toneladas con cada lanzamiento y planeaban darle a Europa una abrumadora supremacía en el negocio de comercio espacial.

Todo lo que tomó para explotar ese cohete en menos de un minuto en su primer viaje el junio pasado, dispersando escombros cerca de los pantanos de manglares de la Guayana Francesa, fue un pequeño programa de computadora tratando de meter un número de 64 bits en un espacio de 16 bits.

Un error, una explosión. De todas las líneas de código sin cuidado grabadas en los anales de las ciencias computacionales, esta puede quedarse como una de las más eficientemente devastadores. De las entrevistas con expertos en cohetes y de un análisis preparado para la agencia espacial, emerge un camino despejado para un error aritmético que conduce a la destrucción total.

*Fragmento de la caída del lanzamiento fallido de Ariane 501.*

Para reproducir la grabación en retrospectiva:

39 segundos después del lanzamiento, mientras el cohete alcanzaba una altitud de dos millas y media, un mecanismo de autodestrucción terminó con Ariane 5, junto con su carga útil de cuatro satélites científicos no asegurados y de gran valor monetario. El mecanismo de autodestrucción se activó automáticamente debido a que la fuerza aerodinámica estaba desprendiendo los propulsores del cohete.

Esta desintegración había empezado un instante antes, cuando la nave espacial se desvió de su curso bajo la presión de tres poderosos inyectores que estaban en los propulsores y el motor. El cohete estaba haciendo una corrección abrupta de curso que no se requería, compensando por una vuelta incorrecta que no había pasado.

El volante estaba controlado por la computadora a bordo, misma que pensó que el cohete necesitaba una corrección de curso debido a los números que venían del sistema de guía inercial. El sistema usa giroscopios y acelerómetros para rastrear el movimiento. Los números se veían como datos de vuelo – datos de vuelo bizarros e imposibles – que en realidad eran un mensaje de error de diagnóstico. El sistema de guía, de hecho se había apagado.

Este apagón ocurrió 36.7 segundos después del lanzamiento, cuando la computadora del sistema de guía trató de convertir una pieza de datos –la velocidad lateral del cohete— de un formato de 64 bits a uno de 16 bits. El número era muy grande y un error por exceso ocurrió, Cuando el sistema de guía se apagó, le pasó el control a una unidad idéntica y redundante, que estaba ahí para proveer refuerzo en caso de justo esa falla. Pero la segunda unidad falló justo en la misma manera unos milisegundos antes. ¿Y por qué no? Estaba corriendo el mismo software.

Este bug pertenece a una especie que ha existido desde que los primeros programadores de computadoras se dieron cuenta de que podían guardar números como secuencias de bits, átomos de datos, unos y ceros: 1001010001101001. . . .

Un bug como este, en un día malo puede provocar un crash a una hoja de cálculo o un procesador de palabras. Ordinariamente, cuando un programa convierte datos de una forma a otra, las conversiones están protegidas por líneas extra de códigos que vigilan para encontrar errores y recuperarlos con gracia. Ciertamente, muchas de las conversiones de datos en la programación del sistema de guía, incluyen esta protección.

Pero en este caso, los programadores decidieron que esta figura de velocidad en particular nunca sería lo suficientemente larga para causar problemas. Después de todo, nunca lo había sido. Desafortunadamente, Ariane 5 era un cohete más rápido que Ariane 4. Una ridiculez extra: el cálculo contenía el bug, que apagó el sistema de guía, que confundió a la computadora a bordo, que forzó al cohete fuera de curso, de hecho, no tenía propósito una vez que el cohete estuviera en el aire. Su única función era alinear el sistema antes del lanzamiento. Así que debieron haberlo apagado. Pero los ingenieros decidieron tiempo atrás, en una versión temprana del Ariane, dejar esta función corriendo los primeros 40 segundos de vuelo – “una característica especial” que estaba dedicada a hacer más fácil reiniciar el sistema en caso de que existiera un atraso breve en la cuenta regresiva.

Los europeos esperaban lanzar un nuevo Ariane 5 la siguiente primavera, esta vez con un nuevo arquitecto de software designado, quien revisará el proceso de una simulación de suelo más intensiva y esperan, realista. La simulación es la gran esperanza de los debuggers de software en todos lados, aunque no pueden anticipar cada posibilidad de la vida real. Jacques Durand, jefe de proyecto, en París, dice que “Los detalles más mínimos pueden tener consecuencias terribles”. “No es una sorpresa, especialmente en un sistema de software tan complejo como lo es este”.

*Puntal de soporte de la estructura del satélite recuperado.*

Estos días, tenemos complejos sistemas de software en todas partes. Los tenemos en nuestros lavaplatos y en nuestros relojes de mano, aunque no son tan críticamente enfocados a una misión. Tenemos computadoras en nuestros carros—de 15 a 50 microprocesores, dependiendo cómo los cuentes: en el motor, la transmisión, las suspensiones, el volante, los frenos y cualquier otro subsistema mayor. Cada uno corre su propio software que ha sido, sin duda, críticamente probado, simulado y debuggeado.

Billl Powers el vicepresidente de investigación en Ford, dice que el poder de computación de un carro está crecientemente devoto a no sólo el control, si no al diagnóstico y los planes de contingencia –“Debería abortar la misión? ¿Y si la aborto a dónde debo ir?” dice. “También tenemos lo que se llama una estrategia de “cojeo a casa”. Eso es, en el peor caso, el carro debería comportarse más o menos normal, como un carro de la era pre-computadora, en vez de, por decir, decidir por sí mismo estrellarse en el árbol más cercano.

Los investigadores europeos eligieron no singularizar como culpable a ningún departamento o contratista particular. “Se tomó una decisión” escribieron. “No fue analizado o completamente entendido”. Y “las posibles implicaciones de permitir que continuara su función durante el vuelo no fueron contempladas”. No intentaron calcular cuánto tiempo o dinero se salvaba mediante la omisión del código estándar de protección de errores.

“El panel desea destacar”, añadieron, con la magnífica insipidez de muchos reportes de accidentes “ese software es una expresión de un diseño altamente detallado y no falla en el mismo sentido de un sistema mecánico”. No. Falla en un sentido diferente. Software que se construyó en años de millones de líneas de código, ramificándose, desdoblándose e entrelazándose, al final resulta comportándose más como un organismo que como una máquina.

“No hay vida en la actualidad sin software”, dice Fran Laza, un ejecutivo vicepresidente del fabricante de cohetes Lockheed Martin. “El mundo probablemente colapsaría”. Afortunadamente, destaca, los softwares realmente importantes tienen una fiabilidad de 99.9999999 por ciento. Al menos, hasta que ya no.

ACCIDENTE MÉTICO CAUSA PÉRDIDA DE ORBITADOR DE LA NASA

El orbitador climático de la Nasa se perdió el 23 de septiembre de 1999.

30 de septiembre de 1999.

Posteado: a las 4:21 p.m. EDT (2021 GMT)

Por Robin Lloyd

Escritor interactivo Senior de CNN

Observador de Marte en la instalación de servicio de carga útil peligrosa.

(CNN)—Nasa perdió un orbitador de Marte de $125 millones, porque un equipo de ingeniería de Lockheed Martin usó unidades inglesas, mientras que el equipo de agencia usó el más convencional, sistema métrico para una operación crucial de nave espacial, de acuerdo a la conclusión de revisión, revelada el martes.

La discrepancia de unidades previno que la información de navegación se transfiriera del equipo del Orbitador Climático de Marte de Lockheed Martin en Denver a el equipo de Laboratorio de Propulsión Jet de la NASA en Pasadena, California.

Lockheed Martin ayudó a construir, desarrollar y operar la nave espacial para la NASA. Sus ingenieros proveyeron comandos de navegación para los propulsores Orbitador Climático en unidades inglesas, aunque NASA ha usado el sistema métrico predominantemente desde, al menos, 1990.

Nadie está apuntando a Lockheed Martin, dijo Tom Galvin, el administrador de JPL (Laboratorio de Propulsión Jet) a quien se reportan todos los gerentes de proyecto.

“Este es un problema de proceso de principio a fin”, dijo. “Un solo error como este no debería haber causado la pérdida del Orbitador Climático. Algo pasó en nuestro proceso de sistema en balances, que debimos haber visto y arreglado.”

El descubrimiento vino de un panel interno de revisión de JPL que reportó la causa a Gavin el miércoles. El grupo incluía cerca de 10 especialistas de navegación, muchos de los cuales se habían retirado de JPL.

“Han estado analizando esto desde la mañana del viernes siguiente a la pérdida”, dijo Gavin.

La discrepancia de navegación mató la misión en un día que los ingenieros estaban esperando celebrar la entrada del equipo en la órbita de Marte.

Después de un viaje de 286 días, la sonda encendió su motor el 23 de septiembre para lanzarse a sí misma en órbita.

*El Orbitador climático de Marte en una prueba de acústica.*

El motor se encendió, pero la nave se encontraba a 60 kilómetros (36 millas) del planeta – cerca de 100 kilómetros más cerca de lo que se había planeado y cerca de 25 kilómetros (15 millas) debajo del nivel al cual podía funcionar propiamente, dijeron los miembros de la misión.

Los últimos descubrimientos, mostraron que la propulsión del sistema de la nave se sobrecalentó y se deshabilitó mientras el Orbitador Climático entraba profundamente en la atmósfera, dijo Frank O´Donell, un comunicador de JPL.

Eso probablemente detuvo al motor de quemarse por completo, por lo que el orbitador atravesó la atmosfera, continuando más allá de marte y probablemente ahora se encuentra orbitando el sol, comentó.

El orbitador climático iba a proveer datos para otra misión llamada aterrizador polar de marte, que se planeaba llevar a cabo en marte en diciembre. Ahora los planificadores están trabajando en cómo obtener datos a través de su propia radio y otro orbitador que orbita el planeta rojo.

El orbitador climático y el aterrizador polar fueron diseñados para ayudar a científicos a entender la historia del agua en marte y el potencial de vida en el pasado del planeta. Hay fuerte evidencia de que marte contenía agua, pero los científicos no tienen una respuesta clara a dónde se fue el agua de marte.

La nasa ha llevado a cabo dos paneles para investigar qué los llevó a la pérdida del orbitador, incluyendo el panel interno de revisión por pares que publicó el jueves. La nasa también planea formar un tercer panel para investigar el accidente.

El sistema métrico utilizado por la NASA desde hace años.

Un documento de la NASA fue publicado hace años, donde la misión del Cassini a saturno fue desarrollada, estableciendo el sistema métrico para todas las unidades de medición, comentó Gavin.

El sistema métrico es usado para la misión del aterrizador polar, así como en la próxima misión a marte, comentó.

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

"Vamos a ver cómo se transfirieron los datos", dijo Gavin. "¿Cómo entró originalmente en sistema en unidades inglesas? ¿Cómo se transfirió? Cuando hacíamos navegación y Doppler (distancia y velocidad) controles, ¿cómo es que no lo encontramos?"

"La gente comete errores", dijo Gavin. "El problema aquí no fue el error. Fue el fracaso de nosotros para mírarlo de extremo a extremo y encuéntralo. Es injusto depender de una sola persona". Lockheed Martin, que no devolvió de inmediato una llamada telefónica para hacer comentarios, está construyendo orbitadores y módulos de aterrizaje para futuras misiones a Marte, incluido uno que se lanzará en 2001 y una misión eso devolverá algunas rocas de Marte a la Tierra dentro de unos años.

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

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

Causa del fracaso.

El 10 de noviembre de 1999, la Junta de Investigación de Accidentes del Orbitador Climático de Marte publicó una Fase I informe, que detalla los problemas sospechosos encontrados con la pérdida de la nave espacial.

Previamente, 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. Se pretendía colocar la nave espacial en una posición óptima para una maniobra de inserción que llevaría a la nave espacial alrededor de Marte a una altitud de 226 kilómetros el 23 de septiembre de 1999. Sin embargo, durante la semana entre TCM-4 y la inserción orbital maniobra, el equipo de navegación indicó que la altitud puede ser mucho más baja que la prevista en 150 a 170 kilómetros. Veinticuatro horas antes de la inserción orbital, los cálculos colocaron al orbitador en una altitud de 110 kilómetros; 80 kilómetros es la altitud mínima a la que se encontraba Mars Climate Orbiter.

Se cree que es capaz de sobrevivir durante esta maniobra. Los cálculos posteriores a la falla mostraron que la nave espacial estaba en una trayectoria que habría llevado al orbitador a 57 kilómetros de la superficie, donde la nave espacial probablemente se desintegró debido a las tensiones atmosféricas.

La causa principal de esta discrepancia fue que una pieza de software de tierra proporcionada por Lockheed Martin produjo resultados en una unidad consuetudinaria de los Estados Unidos ("American"), contrariamente a su Software Especificación de interfaz (SIS), mientras que un segundo sistema, suministrado por la NASA, que utilizó esos resultados esperaba que estuvieran en unidades métricas, de acuerdo con el SIS. Software que calculó el total.

El impulso producido por los disparos del propulsor se calcula en libras-segundo. El cálculo de la trayectoria usó estos resultados para corregir la posición predicha de la nave espacial por los efectos del propulsor despidos. Este software esperaba que sus entradas estuvieran en newton-segundos.

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