O Boletim SBMAC divulga uma versão condensada do relatório sobre a falha no primeiro lançamento do Ariane 5, em parte baseada no texto do SIAM News, V29 N.8, out/96.

ARIANE 5: UM ERRO NUMÉRICO (*OVERFLOW*) LEVOU À FALHA NO PRIMEIRO LANÇAMENTO

Tradução de José Nivaldo Hinkel

Fonte desta Imagem

Em 4 de junho de 1996, menos de um minuto após o lançamento, o foguete francês Ariane 501 se autodestruiu. Era o primeiro lançamento da série Ariane 5 e, logo em seguida, foi indicada pelo CNES (Centro Nacional de Estudos Espaciais) e pela ESA (Agência Espacial Européia) uma comissão presidida pelo matemático francês Jacques-Louis Lions, do Colégio de França, para investigar a ocorrência.

A avaliação dessa comissão indica um erro no *software* de controle como a origem na falha do lançamento. O presente resumo se baseia no relatório dessa comissão, concluído seis semanas após o acidente

O ACIDENTE

Com base na documentação disponível à comissão, conclui-se que as condições meteorológicas na base de lançamento em Kourou, Guiana Francesa, na manhã de 4 de junho de 1996, eram aceitáveis para o lançamento. Em particular, não havia riscos de relâmpagos e a intensidade do campo elétrico medida na base foi considerada desprezível. A única incerteza restringia-se ao critério de visibilidade considerado não totalmente satisfatório.

A contagem regressiva avançou sem problemas até 7 minutos antes do instante previsto para o lançamento, quando foi suspensa, por ser o critério de visibilidade avaliado "definitivamente insatisfatório". Conforme fora previsto, entretanto, essas condições melhoraram mais tarde, permitindo a retomada da contagem regressiva. A ignição do motor *Vulcan* e dos dois "*boosters*" transcorreu normalmente, conduzindo à decolagem. O vôo prosseguiu conforme os prognósticos até aproximadamente 37 segundos após a decolagem, quando o veículo se desviou bruscamente do curso previsto, partiu-se e explodiu. Uma investigação preliminar dos dados de vôo revelou:

- **Comportamento do lançador conforme condições nominais, até 36 segundos após a decolagem.**
- **Falha do sistema de referência inercial secundário, seguido imediatamente de falha do sistema de referência inercial em operação.**
- **Guinada dos bocais dos "*boosters*" sólidos até o seu ângulo máximo e, logo a seguir, manobra semelhante do motor *Vulcan* causando uma guinada abrupta do veículo**

- **Autodestruição do lançador, disparada corretamente como conseqüência da ruptura das juntas entre os "*boosters*" sólidos e o primeiro estágio..**

A origem da falha foi, dessa forma, rapidamente confinada ao sistema de controle, mais especificamente, aos dois sistemas referenciais inerciais (SRI), que nitidamente deixaram de funcionar quase simultaneamente, por volta de 36,7 segundos após a decolagem.

INFORMAÇÃO DISPONÍVEL

Foram disponibilizados à comissão dados de telemetria recebidos na base terrestre até 42 segundos após a decolagem, dados de trajetória fornecidos por estações de radar, observações óticas (câmeras de infravermelho e óticas) e resultados da inspeção do material recuperado. Os dados de telemetria recebidos em Kourou foram transferidos para o CNES/Toulouse e aí convertidos em gráficos em função do tempo..

A auto-destruição do veículo ocorreu perto da plataforma de lançamento, a uma altitude de aproximadamente 4000 metros. A recuperação dos destroços, espalhados em uma área de aproximadamente 12 quilômetros quadrados, foi dificultada por ser a região pantanosa ou coberta de savana. Mesmo assim, foi possível recolher os dois SRIs no meio dos destroços. De particular interesse foi aquele que deixou de funcionar por último. Ele carregava alguns dados de telemetria que não estavam disponíveis (programou-se a transmissão destas informações para a estação terrestre apenas para a unidade que falhasse primeiro). Os resultados do exame dessa unidade foram muito úteis na análise da seqüência da falha.

De modo geral, podemos dizer que o sistema de controle de vôo do Ariane 5 não tem muita novidade, segue o padrão normal de projetos desta natureza. A atitude do veículo e seus movimentos no espaço são estimados por um SRI. Ele possui computador interno próprio que calcula os ângulos e velocidades com base nas informações oriundas da plataforma inercial contendo giroscópios a laser e acelerômetros. Os dados do SRI são transmitidos por barramento de dados para o computador de bordo(OBC), que executa o programa de vôo e controla os bocais dos "*boosters*" sólidos e do motor criogênico *Vulcan*, por meio de servoválvulas e atuadores hidráulicos.

Para aumentar a confiabilidade há grande redundância a nível de equipamento. Dois SRIs operam em paralelo, com *hardware* e *software* idênticos. Enquanto um deles está operando, o outro permanece em *stand-by*; caso o computador de bordo detete uma falha no SRI em operação, ele imediatamente comuta

para a unidade reserva, desde que esta esteja funcionando corretamente. Da mesma forma, há dois OBCs, e várias outras unidades do sistema de controle de vôo têm suas reservas. O projeto do SRI usado no Ariane 5 é quase idêntico ao do Ariane 4, particularmente no que diz respeito ao *software*.

CONCLUSÕES INICIAIS

Com base na farta documentação e dados disponíveis à comissão, a seguinte cadeia de eventos foi estabelecida, partindo da destruição do veículo e regredindo no tempo em busca do evento iniciador da seqüência.

O veículo começou a desintegrar-se aproximadamente 39 segundos após a decolagem por causa da elevada carga aerodinâmica provocada pelo ângulo de ataque superior a 20 graus, o que levou à separação dos "*boosters*" sólidos com o primeiro estágio do veículo, o que por sua vez disparou o mecanismo de autodestruição do foguete.

Este ângulo de ataque foi causado pela deflexão até ao limite dos bocais dos "*boosters*" sólidos e do motor *Vulcan*.

As deflexões dos bocais foram comandadas pelo OBC com base nos dados transmitidos pelo SRI em operação (SRI 2). Parte dos dados naquele instante não eram realmente dados de vôo, pelo contrário, constituíam uma seqüência de *bits* de diagnóstico do computador do SRI 2, a qual foi interpretada como dados de vôo.

O SRI 2 não enviou os dados corretos de atitude porque a unidade havia declarado uma falha provocada por uma anomalia na execução do *software*.

O computador de bordo não poderia comutar para o SRI reserva (SRI 1) porque aquela unidade já havia deixado de funcionar durante o ciclo anterior (período de 72 mili-segundos) pela mesma razão que o SRI 2.

A anomalia interna de *software* do SRI ocorreu durante a execução de uma conversão de dados de um número de 64 *bits* em ponto flutuante para um inteiro de 16 *bits* com sinal. O valor do número em ponto flutuante era maior do que poderia ser representado pelo inteiro de 16 *bits* com sinal. O resultado foi um operando inválido. A instrução de conversão de dados (em código ADA) não estava protegida contra erros de operando, embora outras conversões de variáveis equivalentes no mesmo segmento de código estivessem protegidas.

O erro ocorreu num segmento do *software* que controla apenas o alinhamento da plataforma inercial. Os resultados fornecidos por este segmento do código são relevantes apenas antes da decolagem. Após a decolagem esta função não serve para nada. A função de alinhamento opera por 50 segundos após o início do modo de vôo dos SRIs (3 segundos antes da decolagem para o Ariane 5). Conseqüentemente, após a decolagem a função continua atuando por aproximadamente 40 segundos de vôo. Esta seqüência temporal é baseada num requisito do Ariane 4 que não faz parte da especificação do Ariane 5.

O erro de operando ocorreu devido a um valor inesperadamente elevado de uma função de alinhamento interno, denominada BH (horizontal *bias*), que está relacionada com a componente horizontal da velocidade monitorada pela plataforma. Este valor é calculado como um indicador de precisão de alinhamento ao longo do tempo. O valor de BH foi muito maior do que o previsto porque o segmento inicial da trajetória do Ariane 5 difere da trajetória do Ariane 4 e resulta em valores

consideravelmente altos para a componente horizontal da velocidade.

Os eventos internos do SRI que originaram a falha foram reproduzidos por simulação computacional. Além disso, ambos os SRIs foram recuperados durante a investigação da comissão e o contexto da falha foi determinado com precisão por meio da leitura dos dados na memória. Tendo a comissão examinado o código do *software*, concluiu que este é consistente com o cenário da falha.

A comissão julga portanto que ficou estabelecido, sem sombra de dúvidas, que a cadeia de eventos estabelecida acima reflete as razões técnicas da falha.

COMENTÁRIOS SOBRE O CENÁRIO DA FALHA

No cenário da falha, as razões primárias são o erro de operando que ocorreu na conversão do valor representando a velocidade horizontal e a falta de proteção dessa conversão, o que implicou na suspensão do funcionamento do computador do SRI.

A comissão foi informada de que nem todas as conversões foram protegidas porque uma carga máxima de 80% fora estabelecida como meta para o computador do SRI. Para determinar a vulnerabilidade do código não protegido, uma análise tinha sido efetuada em cada operação que pudesse causar uma anomalia, incluindo um erro de operando. Em particular, a conversão de ponto flutuante para inteiros foi analisada; operações envolvendo sete variáveis apresentaram risco de provocar erros de operando. Isto ocasionou a adição de proteção a 4 variáveis, como se pode observar no código ADA. Contudo, 3 das variáveis foram deixadas desprotegidas. Nenhuma referência direta que pudesse justificar esta decisão foi encontrada no código fonte. Considerando a farta documentação disponível associada a qualquer aplicação industrial, a hipótese, mesmo tendo sido aprovada, permaneceu essencialmente obscura e isenta de qualquer análise externa.

As três variáveis restantes, incluindo aquela que representava a velocidade horizontal, não estavam protegidas porque considerações adicionais indicaram que seu valor era fisicamente limitado ou que havia uma larga margem de segurança - raciocínio que no caso da variável BH se mostrou incorreto.

Não há evidências de que qualquer dado de trajetória tenha sido utilizado para analisar o comportamento das variáveis não protegidas, e é ainda mais importante notar que foi decidido de comum acordo não incluir dados da trajetória do Ariane 5 nos requisitos e especificação dos SRIs.

Apesar de ter sido identificado que houve um erro de operando, isto por si só não levou à falha da missão. O mecanismo de tratamento de anomalias também contribuiu para a falha. No caso de uma anomalia de qualquer espécie, de acordo com a especificação do sistema, o erro deveria ser indicado no barramento de dados, o contexto do erro deveria ter sido armazenado numa memória EEPROM (que foi recuperada e lida para o Ariane 5), e finalmente, o processador SRI deveria ter parado de funcionar. A decisão de interromper a operação do processador mostrou-se fatal. Reinicilização não é factível porque é muito difícil recalcular a atitude após a parada do processador; portanto, o SRI torna-se sem utilidade nenhuma. A razão subjacente a esta drástica ação encontra-se na prática comum do programa Ariane de tratamento apenas das falhas aleatórias de *hardware*. Utilizando este raciocínio, anomalias ou mecanismos de manipulação de erros são projetados para falhas aleatórias de *hardware*, os quais podem ser racionalmente tratados por um sistema de reserva.

CRÍTICAS INICIAIS

Apesar de ter sido a falha provocada por um erro sistemático de projeto do *software*, mecanismos poderiam ter sido introduzidos para diminuir este tipo de problema. Por exemplo, os computadores internos dos SRIs poderiam ter continuado a fornecer sua melhor estimativa sobre a atitude requerida. É estranho que por uma anomalia de *software* seja permitida, ou mesmo exigida, uma parada do processador enquanto ele está controlando um equipamento crítico de vôo.

O requisito original responsável pela operação continuada do *software* de alinhamento após a decolagem foi estabelecido há mais de 10 anos para os primeiros modelos do Ariane, com a finalidade de sobreviver a eventos extremamente improváveis de interrupção na contagem regressiva, por exemplo, em T-9 segundos, quando inicia o modo de vôo no SRI do Ariane 4 e, T+5 segundos, quando a reinicialização de certos eventos originados no lançador levariam diversas horas. O período escolhido para a continuação desta operação de alinhamento, 50 segundos após o início do modo de vôo, foi baseado no tempo necessário para o equipamento de terra assumir o controle do veículo no caso de uma interrupção do lançamento.

Esta função especial permitiu nas versões anteriores do Ariane reiniciar a contagem regressiva sem ter que esperar o alinhamento normal, o qual demora 45 minutos ou mais, de forma que uma estreita janela de lançamento possa ser utilizada. De fato, esta função foi utilizada uma vez em 1989.

O mesmo requisito não se aplica ao Ariane 5, que tem uma seqüência de preparação diferente, e foi mantida por razões de consenso, presumivelmente com base no fato de que, a menos que seja comprovadamente necessário, não seria recomendável promover mudanças em um *software* que funcionou bem no Ariane 4.

Mesmo em casos em que a exigência ainda seja considerada válida, seria questionável que a operação de alinhamento operasse após a decolagem. O alinhamento de plataformas mecânicas e lasers precintados envolve o uso de funções matemáticas complexas de filtragem para o alinhamento adequado do eixo *x* com o eixo gravitacional e a determinação do norte a partir do movimento de rotação da Terra. A hipótese de alinhamento antes do vôo considera que o lançador esteja fixo numa posição conhecida. Portanto a função de alinhamento é completamente perturbada quando executada durante o vôo. Os movimentos medidos do lançador são interpretados como *offset* de sensores e outros coeficientes caracterizando comportamentos dos sensores.

CONCLUSÕES FINAIS

Retornando ao erro de *software* - *software* é a expressão de um projeto detalhadamente elaborado e não admite falhas como sistemas mecânicos. Além disso, linguagens de *software* são altamente flexíveis e expressivas, e dessa forma podem solicitar requisitos exigentes, que por sua vez levem a implementações complexas e de difícil validação.

Um tema subjacente ao desenvolvimento do Ariane 5 é a tendência ao alívio de falhas eletrônicas. O fornecedor do SRI seguiu as especificações que lhe foram impostas, as quais exigiam que, no caso de deteção de qualquer anomalia, o funcionamento do processador deveria ser interrompido. A anomalia ocorrida não foi devida a um erro aleatório e sim a um erro de projeto. A anomalia foi detetada mas foi tratada inadequadamente porque havia sido adotado o ponto de vista de que o *software* deveria ser considerado correto até demonstrado o contrário. A comissão tem razões para acreditar que tal ponto de vista é utilizado também em outras áreas de projeto de *software* do Ariane 5. A comissão é de opinião contrária - o *software* é considerado apto a falha enquanto não for avaliado com os métodos mais poderosos para demonstrar sua confiabialidade.

Isto significa que *software* crítico - no sentido de que uma falha por ele provocada pode por em risco a missão - deve ser submetido a níveis de identificação muito detalhados, que comportamentos anômalos devem ser confinados e que uma estratégia confiável de suporte deve levar em consideração as falhas de *software*.

Tradução de José Nivaldo Hinkel
Divisão de Mecânica e Controle
MCT/INPE
São José dos Campos - SP