Всем добрый день, сегодня бы хотел рассказать вам об Аварии ракеты носителя Ариан-5.

Начнем немного с предыстории.

Ариан-5 – это европейская одноразовая ракета-носитель которая входит в семейство Ariane первый запуск которых состоялся еще в 1979 году. Семейство этих ракет используется для вывода на околоземную орбиту средних или тяжелых космических аппаратов. Одновременно в данной ракете может находится 2-3 спутника и попутно до 8 микроспутников.

Первый запуск Ариан-5 состоялся 4 июня 1996 года в 9 часов 33 минуты 59 секунд местного времени. Через 36 секунд после старта когда ракета находилась на высоте 3700 метров, она внезапно отклонилась от запланированной траектории, начала разваливаться и уже на 40-ковой секунде взорвалась.

Предыдущая модель ракета Ариан-4 успешно запускалась более 100 раз, так что же пошло не так с ракетой Ариан-5? Попробуем разобраться.

**Для начала нужно узнать о технической составляющей нашей ракеты.**

Положение и ориентация ракеты-носителя в пространстве измерялись Навигационной Системой (Inertial Reference Systems — IRS), составной частью которой является встроенный компьютер, вычисляющий углы и скорости на основе информации от бортовой Инерциальной Платформы, оборудованной лазерными гироскопами и акселерометрами. Данные от IRS передавались по специальной шине на Бортовой Компьютер (On-Board Computer — OBC), который обеспечивал необходимую для реализации программы полета информацию и непосредственно — через гидравлические и сервоприводы — управлял твердотопливными ускорителями и криогенным двигателем типа Вулкан (Vulkain). Для обеспечения надежности Системы Управления Полетом использовалось **дублирование оборудования**. Поэтому две системы IRS (одна — активная, другая — ее горячий резерв) с идентичным аппаратным и программным обеспечением функционировали параллельно. Как только бортовой компьютер OBC обнаруживал, что «активная» IRS вышла из штатного режима, он сразу же переключается на другую. Бортовых компьютеров тоже было два.

**Значимые Фазы развития процесса.**

За 7 минут до запланированного старта было зафиксировано нарушение «критерия видимости». Поэтому старт был перенесен на час.  
  
И вот наступает тот самый раковой момент t=9 час. 33 мин. 59 сек. местного времени «окно запуска» было вновь «поймано» и был, наконец, осуществлен сам запуск, который и происходил штатно вплоть до момента t+37 секунд.

В последующие секунды произошло резкое отклонение ракеты от заданной траектории, что и закончилось взрывом.

В момент H0+39 секунд из-за высокой аэродинамической нагрузки вследствие превышения «углом атаки» критической величины на 20 градусов произошло отделение стартовых ускорителей ракеты от основной ее ступени, что и послужило основанием для включения Системы Автоподрыва ракеты.

Изменение угла атаки произошло по причине нештатного вращения сопел твердотопливных ускорителей, такое отклонение сопел ускорителей от правильной ориентации вызвала в момент H0 + 37 секунд команда, выданная Бортовым Компьютером на основе информации от активной Навигационной Системы (IRS 2).

Часть этой информации была в принципе некорректной: то, что интерпретировалось как полетные данные, на самом деле являлось диагностической информацией встроенного компьютера системы IRS 2.  
  
Встроенный компьютер IRS 2 передал некорректные данные, потому что диагностировал нештатную ситуацию, «поймав» исключение (exception), выброшенное одним из модулей программного обеспечения.  
  
При этом Бортовой Компьютер не мог переключиться на резервную систему IRS 1, так как она уже прекратила функционировать в течение предшествующего цикла (занявшего 72 миллисекунд) — по той же причине, что и IRS 2.  
  
Исключение, «выброшенное» одной из программ IRS, явилось следствием выполнения преобразования данных из 64-разрядного формата с плавающей точкой в 16-разрядное целое со знаком, что привело к «Operand Error».  
  
Ошибка произошла в компоненте ПО, предназначенном исключительно для выполнения «регулировки» Инерциальной Платформы. Причем этот программный модуль выдает значимые результаты только до момента H0+7 секунд отрыва ракеты со стартовой площадки. После того, как ракета взлетела, никакого влияния на полет функционирование данного модуля оказать не могло.  
  
«Функция регулировки» действительно должна была (в соответствии с установленными для нее требованиями) действовать еще 50 секунд после инициации «полетного режима» на шине Навигационной Системы (момент H0-3 секунд), что она и делала.  
  
Ошибка «Operand Error» произошла из-за неожиданно большой величины BH (Horizontal Bias — горизонтальный наклон), посчитанной внутренней функцией на основании величины «горизонтальной скорости», измеренной находящимися на Платформе датчиками.  
  
Величина BH служила индикатором точности позиционирования Платформы. величина BH оказалась много больше, чем ожидалось потому, что траектория полета Ariane 5 на ранней стадии существенно отличалась от траектории полета Ariane 4 (где этот программный модуль использовался ранее), что и привело к значительно более высокой «горизонтальной скорости».  
  
Финальным же действием, имевшим фатальные последствия, стало прекращение работы процессора. Соответственно, вся Навигационная Система перестала функционировать. Возобновить же ее действия оказалось технически невозможно.  
  
Эту цепь событий удалось полностью воспроизвести с помощью компьютерного моделирования, что — вкупе с материалами других исследований и экспериментов — позволило заключить, что причины и обстоятельства катастрофы полностью выявлены.

**Причины и истоки аварии**

Первоначальное требование на продолжение выполнения операции регулировки после взлета ракеты было заложено более чем за 10 лет до рокового события, когда проектировались еще ранние модели серии Ariane.  
При некотором маловероятном развитии событий взлет мог быть отменен буквально за несколько секунд до старта, например в промежутке H0-9 секунд, когда на IRS запускался «полетный режим», и H0-5 секунд, когда выдавалась команда на выполнение некоторых операций с ракетным оборудованием.  
  
В случае неожиданной отмены взлета необходимо было быстро вернуться в режим «обратного отсчета» (countdown) — и при этом не повторять сначала все установочные операции, в том числе приведение к исходному положения Инерциальной Платформы (операция, требующая 45 мин. — время, за которое можно потерять «окно запуска»).

Однако, Ariane 5, в отличие от предыдущей модели, имел уже принципиально другую дисциплину выполнения предполетных действий — настолько другую, что работа рокового программного модуля после времени старта вообще не имела смысла. Однако, модуль повторно использовался без каких-либо модификаций.

**Язык Ада**

Расследование показало, что в данном программном модуле присутствовало целых семь переменных, вовлеченных в операции преобразования типов. Оказалось, что разработчики проводили анализ всех операций, способных потенциально генерировать исключение, на уязвимость.  
  
Это было их вполне сознательным решением добавить надлежащую защиту к четырем переменным, а три — включая BH — оставить незащищенными. Основанием для такого решения была уверенность в том, что для этих трех переменных возникновение ситуации переполнения *невозможно в принципе*.  
  
Уверенность эта была подкреплена расчетами, показывающими, что ожидаемый диапазон физических полетных параметров, на основании которых определяются величины упомянутых переменных, таков, что к нежелательной ситуации привести не может. И это было верно — но для траектории, рассчитанной для модели Ariane 4.  
  
А ракета нового поколения Ariane 5 стартовала по совсем другой траектории, для которой никаких оценок не выполнялось. Между тем она (вкупе с высоким начальным ускорением) была такова, что «горизонтальная скорость» превзошла расчетную (для Ariane 4) более чем в пять раз.  
  
Защита для всех семи (включая BH) переменных не была обеспечена, потому что для компьютера IRS была продекларирована максимальная величина рабочей нагрузки в 80%. Разработчики должны были искать пути снижения излишних вычислительных издержек и они ослабили защиту там, где теоретически нежелательной ситуации возникнуть не могло. Когда же она возникла, то вступил в действие такой механизм обработки исключительной ситуации, который оказался совершенно неадекватным.  
  
Этот механизм предусматривал следующие три основных действия.

* Информация о возникновении нештатной ситуации должна быть передана по шине на бортовой компьютер OBC.
* Параллельно она — вместе со всем контекстом — записывалась в перепрограммируемую память EEPROM (которую во время расследования удалось восстановить и прочесть ее содержимое).
* Работа процессора IRS должна была аварийно завершиться.

Последнее действие и оказалось фатальным — именно оно, случившееся в ситуации, которая на самом деле была нормальной (несмотря на сгенерированное из-за незащищенного переполнения программное исключение), и привело к катастрофе.

**Вывод**

Дефект на Ariane 5 не был вызван одной причиной. В ходе всей разработки и процессов тестирования существовало много стадий, на которых данный дефект мог быть выявлен.

* Программный модуль был повторно использован в новой среде, где условия функционирования отличались от требований программного модуля. Эти требования не были пересмотрены.
* Система выявила и распознала ошибку. К несчастью, спецификация механизма обработки ошибок была несоответственной и вызвала окончательное разрушение.
* Ошибочный модуль никогда должным образом не тестировался в новом окружении — ни на уровне оборудования, ни на уровне системной интеграции. Следовательно, ошибочность разработки и реализации не была обнаружена.

Авария при запуске привлекла внимание общественности, политиков и руководителей организаций к высоким рискам, связанным с использованием сложных вычислительных систем, что способствовало увеличению инвестирования в исследования, направленные на повышение надежности [систем с особыми требованиями к безопасности](https://en.wikipedia.org/wiki/Life-critical_system). Последующий автоматический анализ кода Ariane стал первым случаем применения [статического анализа](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7_%D0%BA%D0%BE%D0%B4%D0%B0) в рамках крупного проекта с использованием методики [абстрактной интерпретации](https://en.wikipedia.org/wiki/Abstract_interpretation).

**Вопрос:** Было обосновано, что в случае события отмены старта период в 50 секунд после H0-9 будет достаточным для того, чтобы наземное оборудование смогло восстановить полный контроль за Инерциальной Платформой без потери информации — за это время Платформа прекратит начавшееся было перемещение, а соответствующий программный модуль всю информацию о ее состоянии зафиксирует, что поможет оперативно возвратить ее в исходное положение (это в случае, когда ракета продолжает находиться на месте старта).