О программных (и не только) ошибках

Роман Хватов

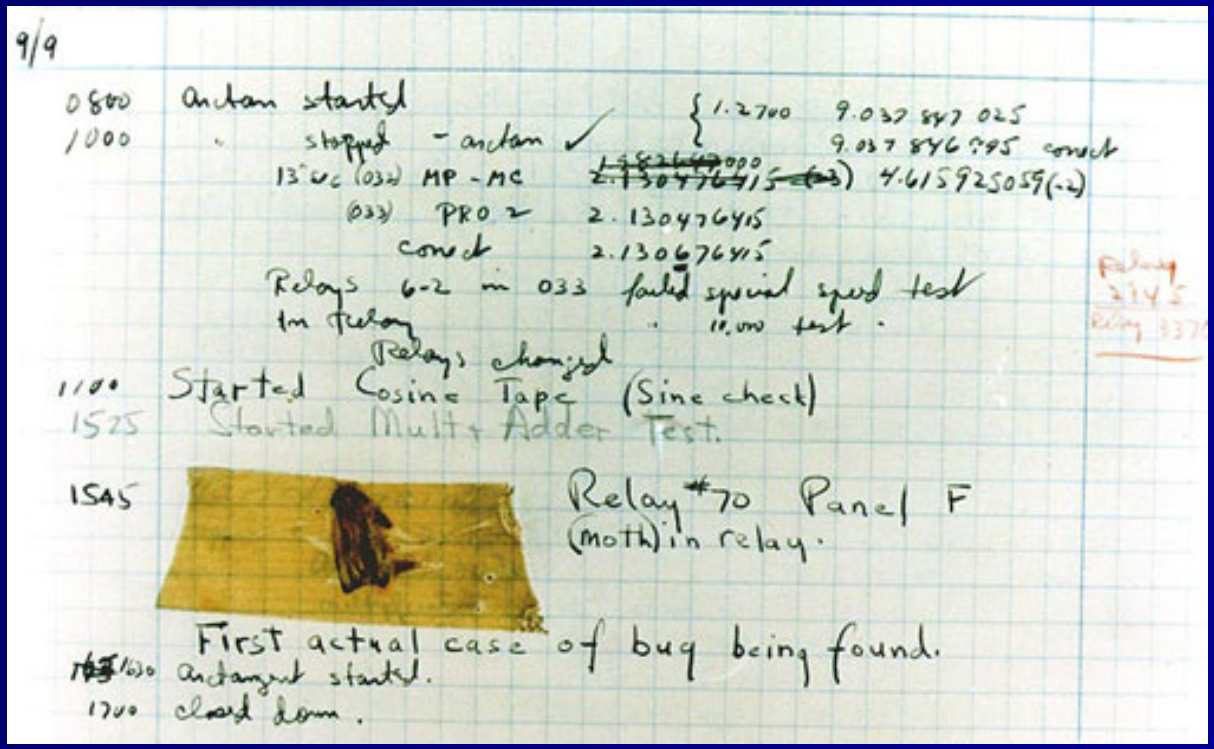
О чем эта лекция

- К чему приводят ошибки
- Как избежать ошибок (правда и заблуждения)
- Неочевидные причины ошибок
- Не только софт
- Еще немного об ошибках ...

Что такое ‘bug’?

1947г, Гарвардский Университет.

Запись в журнале обслуживания компьютера Mark II:



Что такое ‘bug’?

Термин bug появился задолго до 1947г.

Он упоминался в письме Томаса Эдисона к Теодору Пускасу (Theodore Puskas) от 1878г.

Mariner 1

22 Июля 1962г. Взорван через 4:55. Причина катастрофы – опечатка при переносе формулы из тетради в программу

Аппарат для исследования климата Марса (*Mars Climate Orbiter*)

Стартовал 11 декабря 1998.

23 сентября 1999 при выходе на орбиту Марса зашел в тень планеты и уже не вышел.

Конвертоплан Osprey

Испытания 10 декабря 2000г.

Неожиданные действия автоматики при выходе из строя гидравлической системы.

Неожиданные ошибки

- Not enough memory в программе не использующей память
- Magic-More Magic выключатель на PDP 10
- ЭВМ с ‘фотоэффектом’
- Сброс ПО над Мертвым морем
- F22 и «лини перемены дат»
- F16 и экватор

Неожиданные ошибки

- Необычный источник настройки – при изменении частоты с 1111 на 2222 выдавалась последовательность
  - 1111
  - 1112
  - 1122
  - 1222
  - 2222
- Иногда разряды ‘выпадали’:
  - 2222
  - 2022
  - 2222

Ariane 5

4 июня 1996. Взорвалась на 39 секунде полета. Причина – не перехваченное исключение из программного модуля

Что надо делать не всегда

- Переиспользование программных модулей
- Использование ‘надежных’ языков
- Использование exception’ов для сигнализации об ошибках
- Протоколирование ошибок
- Резервное функционирование модулей
- Использовать ограниченность входных данных

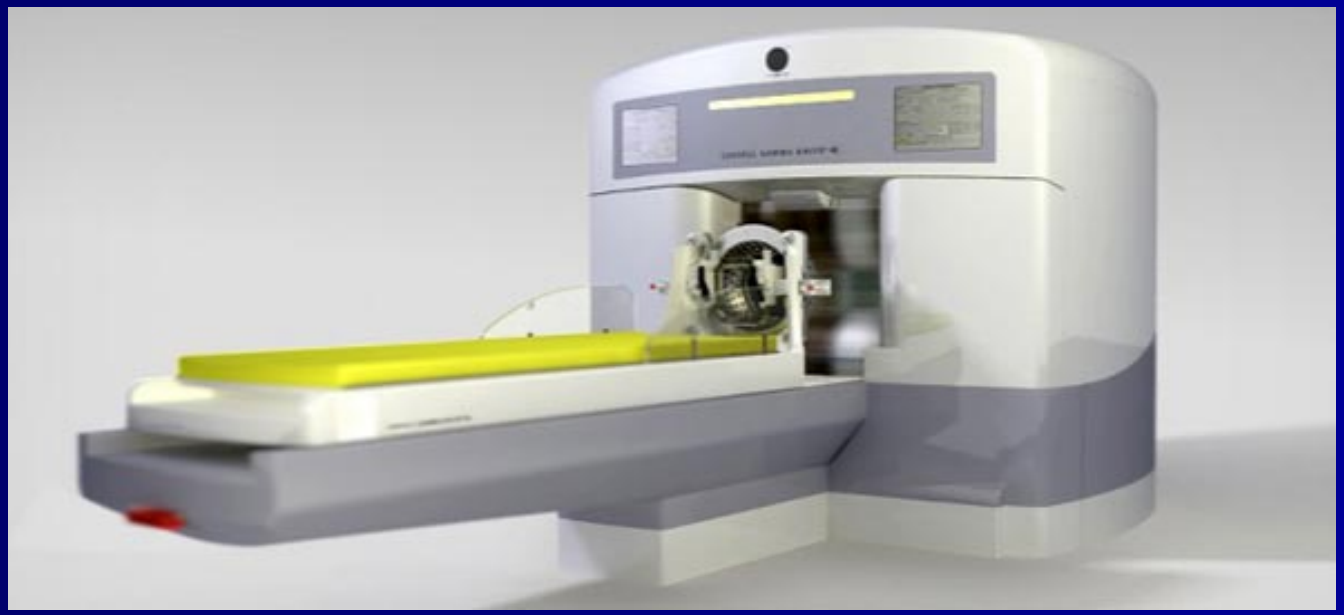
Еще несколько примеров

- Спецификация на ПО тоже может содержать ошибки (Ariane 5)
- Запуск печи бойлера с помощью паяльной лампы
- Попытка внедрить в Англии систему управления воздушным движением

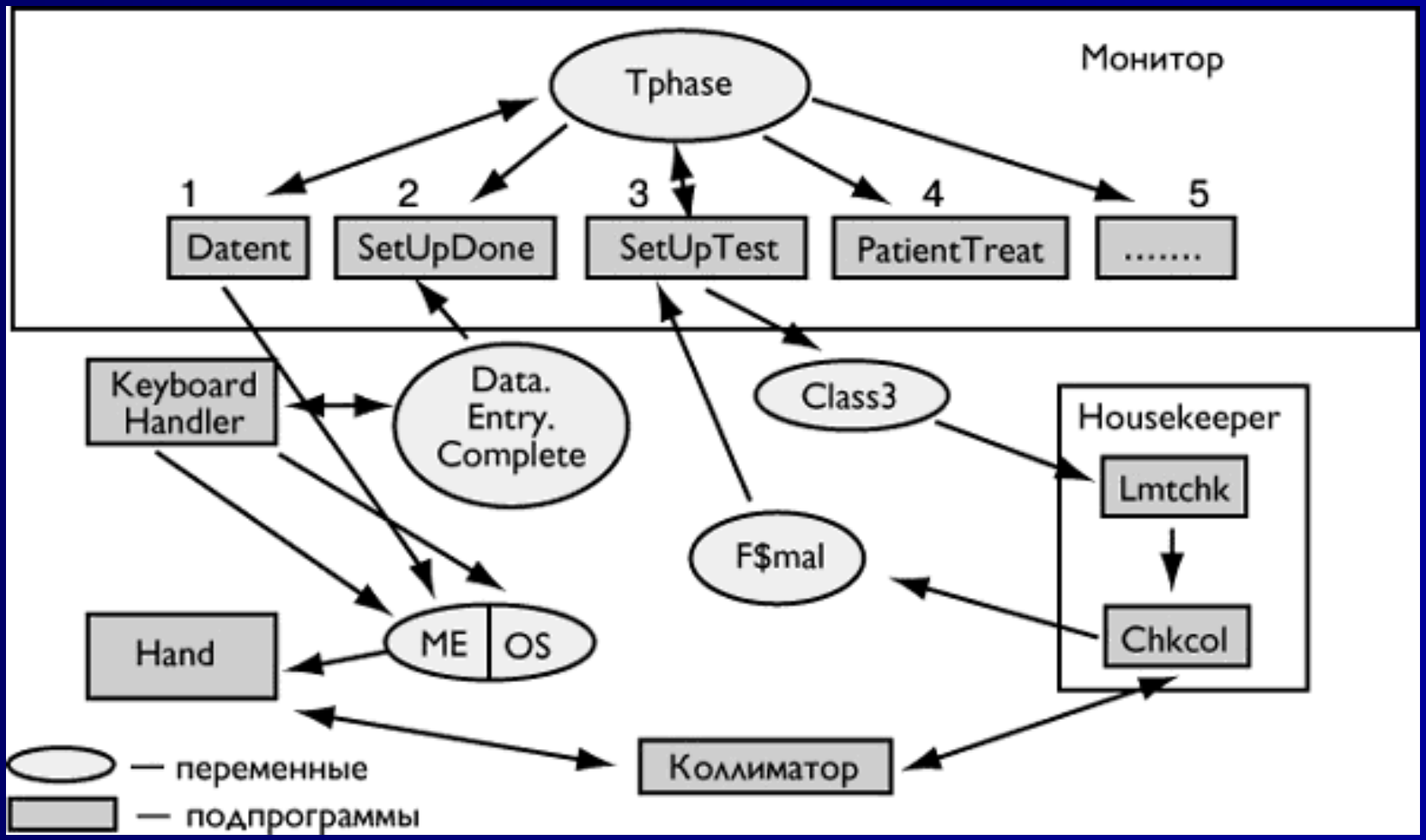
Therac 25

1985-87 гг. 6 человек получили смертельную дозу облучения

Причина – ошибки в синхронизации параллельных процессов



Therac 25


Монитор
Tphase
1
2
3
4
5
Datent
SetUpDone
SetUpTest
PatientTreat
.....
Keyboard Handler
Data. Entry. Complete
Class3
Housekeeper
Lmtchk
F$mal
Chkcol
Hand
ME
OS
Коллиматор
— переменные
— подпрограммы

Что делать надо (и не надо)

- Не переусложняйте систему
- Не забывайте про синхронизацию
- Используйте те данные, которые контролировали
- Используйте аппаратный контроль
- Используйте активные системы контроля

Где нужен активный аппаратный контроль

- Погнутая ось антенны
- Сход с рельсов робота-манипулятора

Multidata Systems Cobalt-60

8 пациентов погибло, еще как минимум 20 получили передозировку.

Multidata Systems была закрыта 7 Мая 2003г FDA комиссией

Ошибка в процессоре Intel Pentium

1993г. Процессор Intel Pentium.

Для некоторых значений операция деления возвращала ошибочные значения (в 5-8 знаке после запятой)

Результат - $475м и невосполнимый ущерб репутации фирмы.

Как реагировать на ошибки?

Руководство по системному программированию Штейнбаха:

> Никогда не выявляйте в программе ошибки, если не знаете, что с ними делать дальше.

- Можно ли добавить обработку ошибок после завершения программы?
- Как реагировать на ошибки?
- Как тестировать программы (coverage, TDD)
- Corner Case ошибки
- UB в программах

Пример UB

```
size_t Hash (const POINT& pt)
{
  return (double)pt.x * 2531011 +
          (double)pt.y * 214013;
}
```

Работала на MSVC 6 и MSVC 2003 и перестала на MSVS 2008 (и на gcc)

Windows Genuine Disadvantage

24 Августа 2007г на WGA сервер была установлена версия с многочисленными ошибками. В следующие 19 часов все экземпляры Windows XP и Windows Vista по всему миру были помечены как нелегальные.

Катастрофическое исследование

5 Февраля 1999г журнал New England Journal of Medicine опубликовал результаты исследования об увеличении количества самоубийств после катастроф.

Из за ошибки в программе, количество самоубийств за последний год было удвоено, что заставило усомнится как в результатах всего исследования так и в репутации самого журнала.

McAfee — перезагрузка

21 Апреля 2010г McAfee распространил обновление вирусной базы №5958. После чего антивирус стал атаковать системный процесс SVCHOST.EXE, что приводило к непрекращающемуся процессу перезагрузки компьютера.

Вертолет Chihook ZD576

В аварии 1994г в Шотландии погибло 29 пассажиров. Причиной аварии стало необычайно низкое качество исполнения одного из программных модулей системы управления.

К вопросу о качестве ПО

- Исследования British Royal Signals and Radar Establishment
- Исследования NASA по программе Shuttle
- EDS Drops Child Support (2004)
- Прекращение проекта ФБР Trilogy (2005)
- Британский паспорт в никуда

M247 Sergeant York

Разработана в начале 80х годов, должна была обеспечить защиту от вертолетов и низколетящих самолетов.

Однако, в связи с выявленными недостатками, программа производства M247 была отменена в 1985 году.

Авария на телефонной компании AT&T

15 Января 1990г все 114 коммутаторов начали периодически перезагружать друг друга каждые 6 секунд. Около 60000 абонентов AT&T не могли никуда позвонить около 9 часов. Результат - $60M.

13 Апреля 1998г в 14:30 в результате замены транк карт, которые оказались неисправными, в коммутаторе Cisco Stratacom BPX, вся сеть вышла из строя. Работа сети смогли восстановить только через сутки.

Ракетный крейсер Yorktown

1996г. В процессе испытаний системы ‘Smart Ship’ крейсер оказался парализован в течении 2:45. Причиной аварии оказался оператор, который записал в поле электронной таблицы значение ноль, которого там не должно было быть.

В результате вышел из строя не только компьютер, где была произведена запись, но и все остальные, входящие в одну сеть.

Озоновая дыра

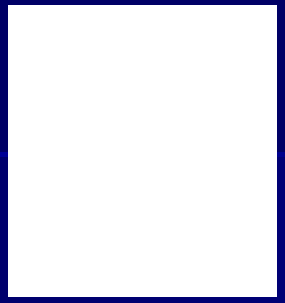
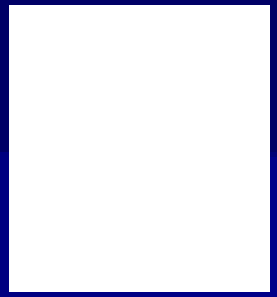
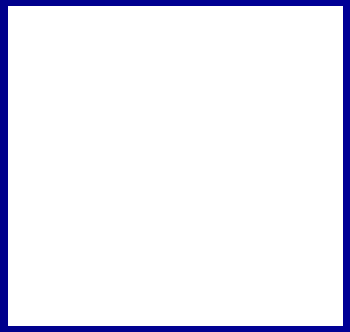
В 1978г NASA запустила проект по раннему обнаружению ‘дыр’ в озоновом слое. Дыра была обнаружена в 1985г и не NASA. Причина была в ПО, которое посчитало отклонение в толщине озонового слоя ошибкой измерения и проигнорировало его.

Ракетный комплекс Patriot

Недостаточная точность отсчета времени (каковая явилась последствием программной ошибки) привела к гибели как минимум 28 солдат.

Коллапс Харфорского Колизея

18 января 1978 года обвалилась крыша спортивной арены не выдержав веса снега. Причиной обрушения стала ошибка проектировщика, который не учел в CAD программе возможный вес снега. Ущерб оценивается в $70M (+ $20M)

	Connection A	Connection B	Connection C	Connection D
Original Design	 Allowable force: 160,000-lb Allowable moment: 0	 Allowable force: 185,000-lb	 Allowable force: 625,000-lb	 Allowable force: 565,000-lb
As-built Design	 Allowable force: 15,440-lb Allowable moment: 9,490 lb-ft	 Allowable force: 59,000-lb	 Allowable force: 363,000- lb	 Allowable force: 565,000-lb

Баг ‘конец света’ (почти)

23 Сентября 1983г на станции раннего обнаружения Серпухов-15 сработала система обнаружения. По ее сведениям США запустили 5 ракет в сторону СССР, что было ошибкой системы распознавания.

Авария в энергосистеме в США и Канаде (2003)

14 августа 2003 года между 15:45 и 16:15, произошло отключение электроэнергии в ряде штатов в США и Канаде.

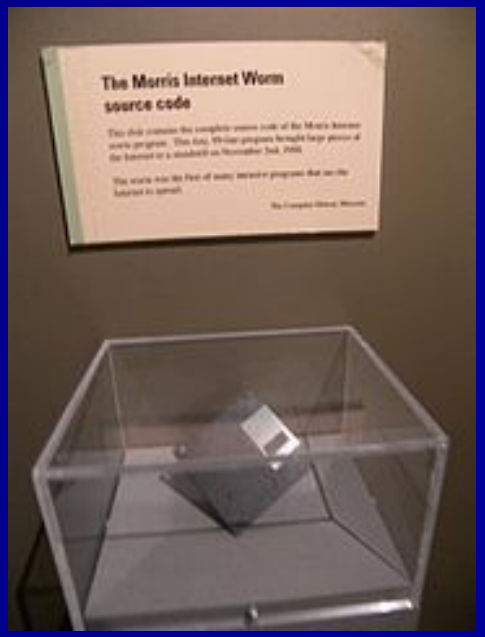
Около 10 млн человек в Канаде (примерно треть населения) и 40 млн — в США остались без электричества.

Денежный ущерб составил

6 миллиардов долларов.

‘Червь’ Морриса

3 Ноября 1988г около 10% всего Интернета было инфицировано ‘червем Морриса’, вызвав практически полный вывод из строя около 6000 машин. Такие последствия не планировались автором, и явились результатом ошибки в самом ‘черве’.



The End ?

Литература

- Мифы о безопасном ПО: уроки знаменитых катастроф
- Летающие глюки
- Northeast blackout of 2003
- The 2003 North American electrical blackout: An accidental experiment in atmospheric chemistry
- Causes of the 2003 Major Grid Blackouts
- Авария в энергосистеме в США и Канаде (2003)

Литература

- History's Worst Software Bugs
- 10 худших багов в истории человечества
- Top Ten Most Infamous Software Bugs Of All Time
- 10 historical software bugs with extreme consequences
- Epic failures: 11 infamous software bugs
- 20 Famous Software Disasters
- Top 10 Costliest Software Bugs

Литература

- Software Failures List
- Изучение знаменитых (и не очень знаменитых) ошибок
- Bell V-22 Osprey
- M247 Sergeant York
- http://forum.vingrad.ru/forum/topic-346611/view-all.html
- http://forum.vingrad.ru/forum/topic-353404/view-all.html
- http://bash.im/quote/417540
- A Story About ‘Magic'

Литература

- USS Yorktown (CG-48)
- Sunk by Windows NT
- Software glitches leave Navy Smart Ship dead in the water
- DiGiorgio denies reported statements
- Smart Ship inquiry a go
- Buggy McAfee update whacks Windows XP PCs
- Morris worm
- With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988
- A Tour of the Worm