Die All Stars der Software Bugs

… und was wir von ihnen lernen können

Christian Seifert
Principal Consultant | esentri AG

christian.seifert@esentri.com
https://team.esentri.com/christian-seifert

9/9

0800 Arctan started { 1.2700 9.037 847 025
1000 " stopped - arctan ✓ 9.037 846 795 correct
13"uc (032) MP - MC ~~1.582649000~~ ~~2.130476415 (-3)~~ 4.615925059(-2)
(033) PRO 2 2.13047 6415
correct 2.13067 6415
Relays 6-2 in 033 failed special speed test
in relay " " 10.00 test.
Relays changed
Relay 2147
Relay 3377
1100 Started Cosine Tape (Sine check)
1525 Started Multy Adder Test.
1545  Relay #70 Panel F
(moth) in relay.
First actual case of bug being found.
~~1525~~ 1630 Arctangent started.
1700 closed down.

Schadenfreude

"Als Schadenfreude wird die Freude über das Missgeschick oder Unglück anderer bezeichnet."

(Wikipedia)

$ 1,5 Billionen

Ja, deutsche Billionen (= 1.500 Milliarden)

Kosten durch "Operational Software Failures" in 2020 alleine in den USA

(Consortium for Information & Software Quality Report)

Die Stars

Mars Climate Orbiter

(1999)

Was war passiert?

Kontakt zur Raumsonde abgebrochen bei Ankunft am Mars

Mars Climate Orbiter

Was war passiert?

$ 327 Millionen Verlust

Was war passiert?

Geplanter Orbit: 150 km

Tatsächlicher Orbit: 57 km

Ursachen

Unterschiedliche Teams für unterschiedliche Teilsysteme

(Lockheed Martin & NASA JPL)

Mars Climate Orbiter

Ursachen

Lockheed Martin verwendete imperiale Einheiten

(Pounds of Force)

NASA verwendete SI Einheiten

(Newton)

Mars Climate Orbiter

Ursachen

Das Kontrollteam erkannte, dass etwas schief läuft

… aber wurde vom Management ignoriert

Lessons to learn

Was können wir für uns mitnehmen?

"uns passiert sowas ja nicht… oder?!"

Mars Climate Orbiter

Lessons to learn

```
public int getTotalAmount();
```

Mars Climate Orbiter

Lessons to learn

```
/**
 * @returns
 *   the total amount the customer should be billed
 *   (in EUR)
 */
public int getTotalAmount();
```

Mars Climate Orbiter

Lessons to learn

```
/**
 * @returns
 *   the total amount the customer should be billed
 */
public int getTotalAmountInEUR();
```

Mars Climate Orbiter

Lessons to learn

```
/**
 * @returns
 *   the total amount the customer should be billed
 */
public MonetaryValue getTotalAmount ();
```

Mars Climate Orbiter

Lessons to learn

```
long lockoutDuration = 57600000;

long lockoutDuration = 16 * 3600000;

long lockoutDuration = 16 * 60 * 60 * 1000;

Duration lockout = Duration.ofHours(16);
```

Mars Climate Orbiter

Lessons to learn

Solides API Design

(z.B. Typen und Value Objects)

Lessons to learn

If you see something:
Do something!

Therac-25

(1980s)

Was war passiert?

Drei Menschen starben nach einer Bestrahlungstherapie durch eine Überdosis

Was war passiert?

Der Hersteller erklärte, der Therac-25 könnte überhaupt keine Überdosis abgeben

… nachdem der Unfall passiert war

Ursachen

Race Condition bei der Dateneingabe

Ursachen

Ein (1) Entwickler

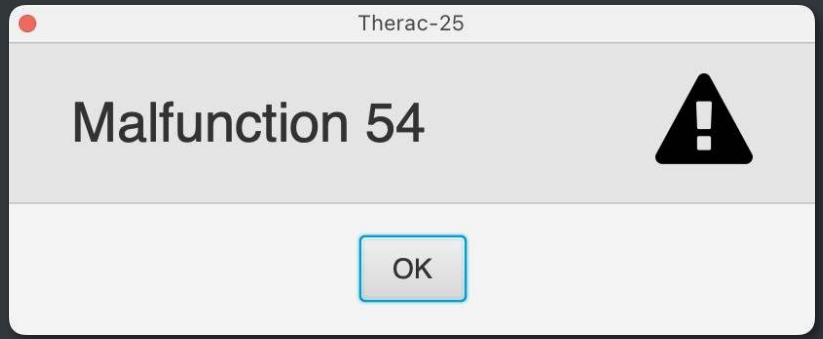
… der gleichzeitig auch für die Qualitätssicherung verantwortlich war

Ursachen

Fehlermedungen wie
"Malfunction 54"
die von Benutzern
nicht verstanden wurden

Therac-25

Ursachen



Therac-25

Lessons to learn

Was können wir für uns mitnehmen?

"uns passiert sowas ja nicht… oder?!"

Lessons to learn

Niemals die Möglichkeit ausschließen, dass der Fehler bei uns liegen könnte

Lessons to learn

Jeder Entwickler ist (zu sehr?) von sich und seinen Fähigkeiten überzeugt

"Das kann doch überhaupt nicht sein!"

Lessons to learn

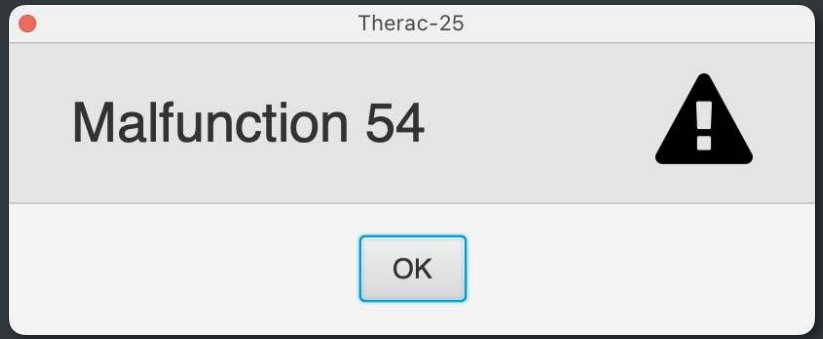
Schutzmaßnahmen in die Organisation mit einbauen

Lessons to learn

Nicht (nur) Fehlermeldungen anzeigen, sondern Details liefern und Optionen anbieten

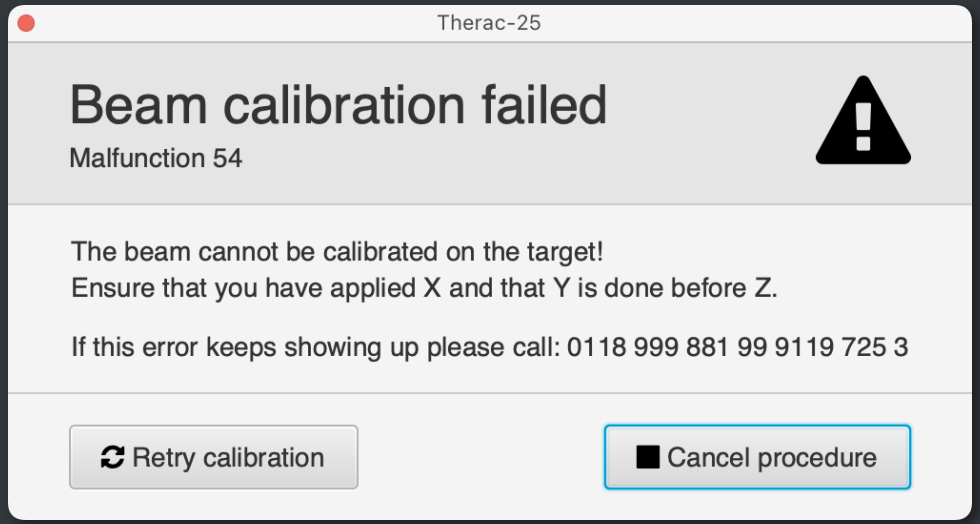
Therac-25

Lessons to learn



Therac-25

Lessons to learn



Ariane 5

(1996)

Ariane 5

Was war passiert?

Was war passiert?

$ 500 Millionen Verlust

Ursachen

Umwandlung eines 64 Bit Floating Point Wertes in einen 16 Signed Integer

… führte zu einem nicht abgefangenen Overflow

Ariane 5

Ursachen

Kein Exception Handling

… und der Overflow war nicht mal missionskritisch
… und das Backup System verwendete den gleichen Code

Ursachen

Große Teile der Steuerungssoftware wurden ohne Anpassungen von der Ariane 4 übernommen

"auf dem letzten Gerät hat's ja auch funktioniert"

Ariane 5

Lessons to learn

Was können wir für uns mitnehmen?

"uns passiert sowas ja nicht… oder?!"

Lessons to learn

Alten Code nicht ungesehen auf neue Probleme loslassen

Ariane 5

Lessons to learn

Defensives Programmieren

(Im Zweifel dann doch noch einen Test mehr erstellen)

Microsoft Zune

(31.12.2008)

Was war passiert?

Nichts

Buchstäblich. Das Gerät reagierte nicht mehr.

Microsoft Zune

Ursachen

Edge Case bei der Datumsberechnung

(31.12.2008)

Microsoft Zune

Ursachen

```
while (days > 365)
{
    if (IsLeapYear(year))
    {
        if (days > 366)
        {
            days -= 366;
            year += 1;
        }
    }
    else
    {
        days -= 365;
        year += 1;
    }
}
```

Microsoft Zune

Ursachen

```
while (days > 365)
{
    if (IsLeapYear(year))
    {
        if (days > 366)
        {
            days -= 366;
            year += 1;
        }
    }
    else
    {
        days -= 365;
        year += 1;
    }
}
```

Microsoft Zune

Ursachen

```
while (days > 365)
{
    if (IsLeapYear(year))
    {
        if (days > 366)
        {
            days -= 366;
            year += 1;
        }
    }
    else
    {
        days -= 365;
        year += 1;
    }
}
```

31.12.2008

days = 366

Microsoft Zune

Ursachen

```
while (days > 365)
{
    if (IsLeapYear(year))
    {
        if (days > 366)
        {
            days -= 366;
            year += 1;
        }
    }
    else
    {
        days -= 365;
        year += 1;
    }
}
```

31.12.2008

`days = 366`

… aber iOS war auch nicht viel besser

(01.01.2012)

iOS

Was war passiert?

Der iOS Wecker funktionierte nicht

(01.01.2012)

Ursachen

Week based year

iOS

Ursachen

2012 Januar	Mo	Di	Mi	Do	Fr	Sa	So
52 2011	26	27	28	29	30	31	1
1 2012	2	3	4	5	6	7	8
2 2012	9	10	11	12	13	14	15
3 2012	16	17	18	19	20	21	22
4 2012	23	24	25	26	27	28	29
5 2012	30	31	1	2	3	4	5

iOS

Ursachen

2012 Januar	Mo	Di	Mi	Do	Fr	Sa	So
52 2011	26	27	28	29	30	31	1
1 2012	2	3	4	5	6	7	8
2 2012	9	10	11	12	13	14	15
3 2012	16	17	18	19	20	21	22
4 2012	23	24	25	26	27	28	29
5 2012	30	31	1	2	3	4	5

iOS

Ursachen

Lockheed Martin F-22 Raptor

(2007)

Lockheed Martin F-22 Raptor

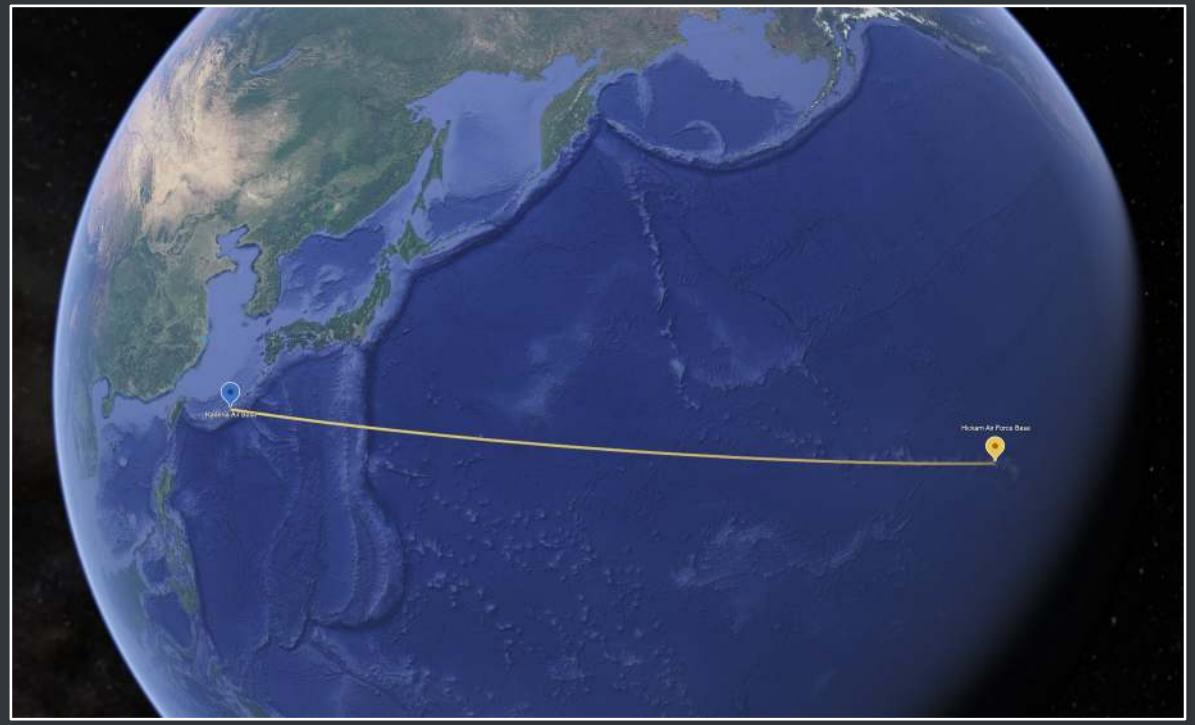
Was war passiert?

Ausfall des Onboard-Computers mitten über dem Pazifik

(Navigation, Kommunikation, …)

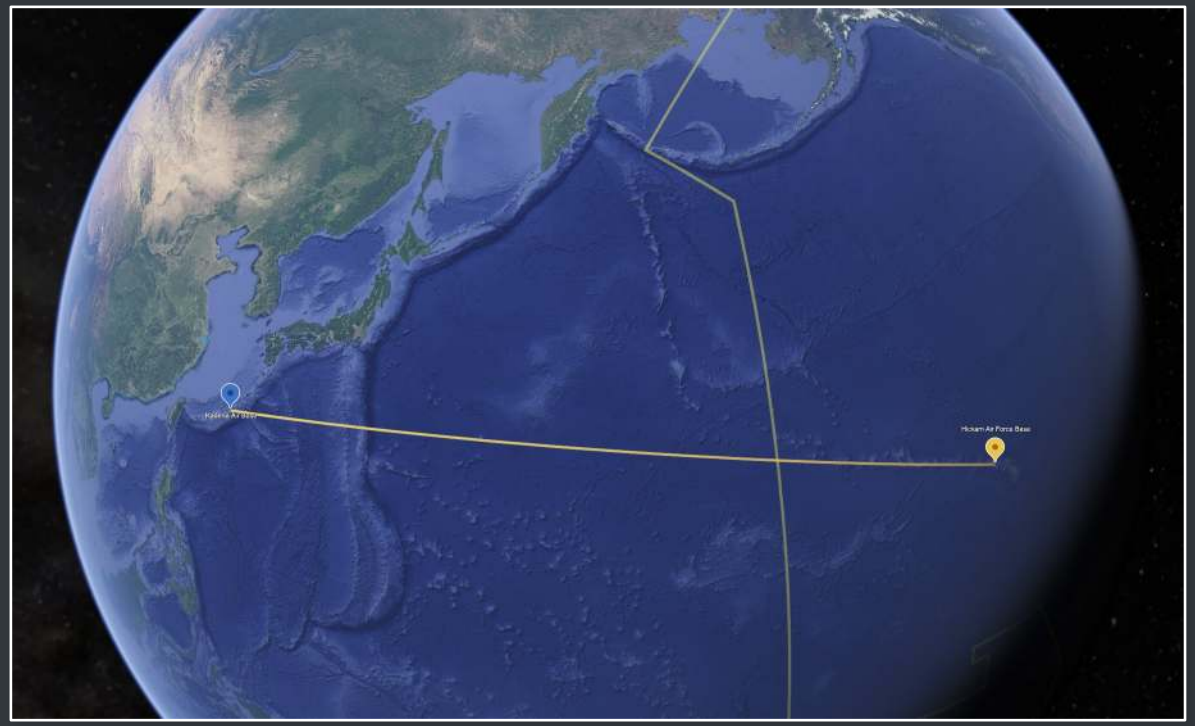
Lockheed Martin F-22 Raptor

Ursachen



Lockheed Martin F-22 Raptor

Ursachen



Microsoft Zune, iOS, Lockheed Martin F-22 Raptor

Lessons to learn

Was können wir für uns mitnehmen?

"uns passiert sowas ja nicht… oder?!"

Microsoft Zune, iOS, Lockheed Martin F-22 Raptor

Lessons to learn

Datums- und Zeitberechnungen sind (immer noch) kompliziert und haben extrem viele Edge Cases

Microsoft Zune, iOS, Lockheed Martin F-22 Raptor

Lessons to learn

Bewährte Tools, Frameworks und Libraries einsetzen und diese (wirklich!) verstehen

Microsoft Windows Genuine Advantage

(2007)

Microsoft Windows Genuine Advantage

Was war passiert?

Valide Lizenzen für Windows XP und Windows Vista wurden als nicht gültig identifiziert

Windows arbeitete nur noch im "Reduced Functionality Mode"

Microsoft Windows Genuine Advantage

Ursachen

Validierungscode zu früh auf Produktionsserver deployed

… an einem Freitag

Ursachen

Die Verschlüsselungskomponenten auf dem Client sollten erst mit dem nächsten Servicepack installiert werden

Ursachen

Problem wurde innerhalb von 30 Minuten erkannt, aber das Rollback dauerte über 12 Stunden!

Microsoft Windows Genuine Advantage

Lessons to learn

Was können wir für uns mitnehmen?

"uns passiert sowas ja nicht… oder?!"

Lessons to learn

Abhängigkeiten berücksichtigen

Microsoft Windows Genuine Advantage

Lessons to learn

Problemsituationen und Ausfälle simulieren und (regelmäßig) testen

Sicherheit in Wiederherstellungsprozessen schaffen

Auf zum Finale…

Boeing 787 Dreamliner

(2020 - ???)

Boeing 787 Dreamliner

Was ~~war passiert~~ ist los?

Flugzeug muss alle 51 Tage neu gebootet werden

Boeing 787 Dreamliner

Ursachen

Historical data accumulates in memory and might lead to "display of misleading data"

Lessons to learn

Ressourcen nicht unnötig in Beschlag nehmen und nach Benutzung wieder aufräumen

Wrapup

9/9

0800 Arctan started { 1.2700 9.037 847 025
1000 " stopped - arctan ✓ 9.037 846 795 correct
13"uc (032) MP - MC ~~1.582649000~~ ~~2.130476415 (-3)~~ 4.615925059(-2)
(033) PRO 2 2.13047 6415
correct 2.13067 6415
Relays 6-2 in 033 failed special speed test
in relay " " 10.00 test.
Relays changed
Relay 2147
Relay 3377
1100 Started Cosine Tape (Sine check)
1525 Started Multy Adder Test.
1545  Relay #70 Panel F
(moth) in relay.
First actual case of bug being found.
~~1525~~ 1630 Arctangent started.
1700 closed down.

Die All Stars der Software Bugs

… und was wir von ihnen lernen können

Christian Seifert
Principal Consultant | esentri AG

christian.seifert@esentri.com
https://team.esentri.com/christian-seifert