The Patriot Missile Failure

Seminar Berühmt-berüchtigte Softwarefehler SS03

Martin Eisemann

Universitaet Koblenz-Landau

Einleitung

On February 25, 1991, a Patriot missile defense system operating at Dhahran, Saudi Arabia, during Operation Desert Storm failed to track and intercept an incoming Scud. This Scud subsequently hit an Army barracks, killing 28 Americans. - General Accounting Office Report Number B-247094

Das Patriot System

Historisches

- Mitte der sechziger gegen sowjetische Flugzeug und Cruise Missile Angriffe in Europa
- Seit Anfang der neunziger auch gegen Short-Range Ballistic Missiles

Historisches

- Hauptaugenmerk lag auf Mobilität und kurzer Einsatzzeit

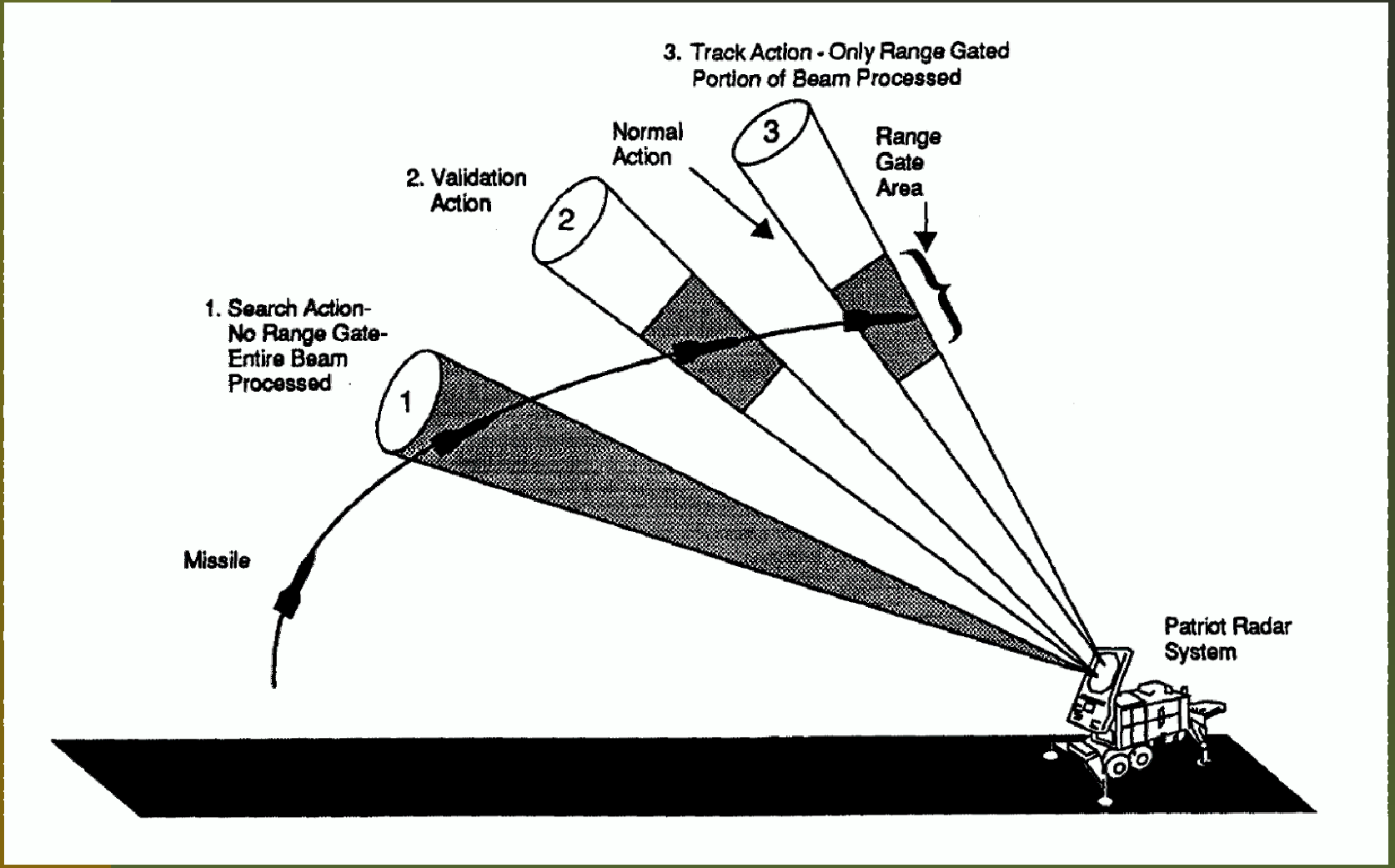
Funktionsweise

- Regelmässige Radarimpulse scannen den Himmel ab
- Gefundene Objekte liefern
  - Breitegrad
  - Längengrad
  - Höhenwinkel (Azimuth)
- Daraus ergeben sich Informationen über
  - Flughöhe
  - Geschwindigkeit
  - Richtung
  - Position

Funktionsweise

- Zielspezifisch
- Range Gate Algorithmus für verdächtige Objekte
- Range Gate Berechnung
- Feuern, falls Objekt in berechneter Range Gate

Funktionsweise



Funktionsweise

- Radar Radius beträgt ca. 70 km
- Irakische SCUD fliegt mit MACH5 (3750 mph)
- Zeitfenster ist eine halbe Minute lang.

Versagen des Patriot System

- Steigernde Unzuverlässigkeit bei andauernder Betriebszeit
- 20% Verschiebung des Range Gates bei acht Stunden Betriebsdauer
- 50% führt zu völligem Versagen, nach etwa 20 Stunden
- System in Dhahran lief bereits über 100 Stunden

Der Fehler – Numerische Probleme

- Range Gate Prediction benötigt unter anderem:
  - Geschwindigkeit
  - Zeitpunkt

Der Fehler – Numerische Probleme

- Geschwindigkeit durch Floating-Point Darstellung
- Zeitpunkt durch ganzzahlige Integer
- 1/10 interner Takt
- Umrechnung Integer zu Float durch Multiplikation mit 0.1

Der Fehler – Numerische Probleme

- $1/10$ entspricht
  $1/2^4 + 1/2^5 + 1/2^8 + 1/2^9 + 1/2^{12} + 1/2^{13}$+... oder
  0.0001100110011001100110011...
- 24 Bit Register Darstellung
  0.000110011001100110011001100

Der Fehler – Numerische Probleme

- Fehler damit proportional zur Betriebsdauer
- Bsp. five digit register counting thirds of seconds (vereinfacht)
  - Bei Beginn

$$\begin{array}{rr} 2 & 0.66667 \\ 1 & \underline{0.33333} \\ & 0.33334 \end{array}$$

Der Fehler – Numerische Probleme

- Fehler damit proportional zur Betriebsdauer
- Bsp. five digit register counting thirds of seconds (vereinfacht)
  - Etwas später

$$\begin{array}{rr} 43 & 14.333 \\ 42 & \underline{14.000} \\ & 0.333 \end{array}$$

Der Fehler – Numerische Probleme

- Fehler damit proportional zur Betriebsdauer
- Bsp. five digit register counting thirds of seconds (vereinfacht)
  - Viel Später

$$\begin{array}{rr} 563 & 187.67 \\ 562 & \underline{187.33} \\ & 0.34 \end{array}$$

Der Fehler – Numerische Probleme

- Bsp. Code:

```
tenth = 1.0 / 10.0;
sec = 100 * 60 * 60 * 10;
t1 = sec * tenth;
t2 = sec/10.0;
output = t2 - t1;
```

(maschinenabhängig)

Der Fehler – Numerische Probleme

- Fehler pro Zehntelsekunde 2^{-20}
- Folge: Radar prüft die falsche Stelle
- Folge: Feindliche Flugkörper werden möglicherweise nicht mehr als solche erkannt.

Der Fehler – Numerische Probleme

- Alpha Batterie in Dhahran bereits über 100 Stunden aktiv
- Fehler:

$$0.0001100110011001100110011001100_2 = \frac{209715}{2097152}$$

$$(\frac{1}{10} - \frac{209715}{2097152})(100*60*60*10) = \frac{5625}{16384} \approx 0.3433 sec$$

Der Fehler – Numerische Probleme

- Eine SCUD fliegt in dieser Zeit über einen halben Kilometer
- Ausserhalb der Range Gate

Der Fehler – Reaktionen

- Fehler war seit 11. Februar 1991 bekannt
- Reaktion der Obrigkeit: *Der normale Patriotbenutzer lässt das System nicht länger als acht Stunden laufen*
- Softwareupdate am 16.Februar losgeschickt
- Am 21. Februar erfolgte Meldung, dass zu lange Betriebszeiten einen Fehler in der Zielerfassung herbeiführen.
- Softwareupdate erreichte Dhahran einen Tag zu spät (Enigma?)

Der Fehler – Die Wahrheit

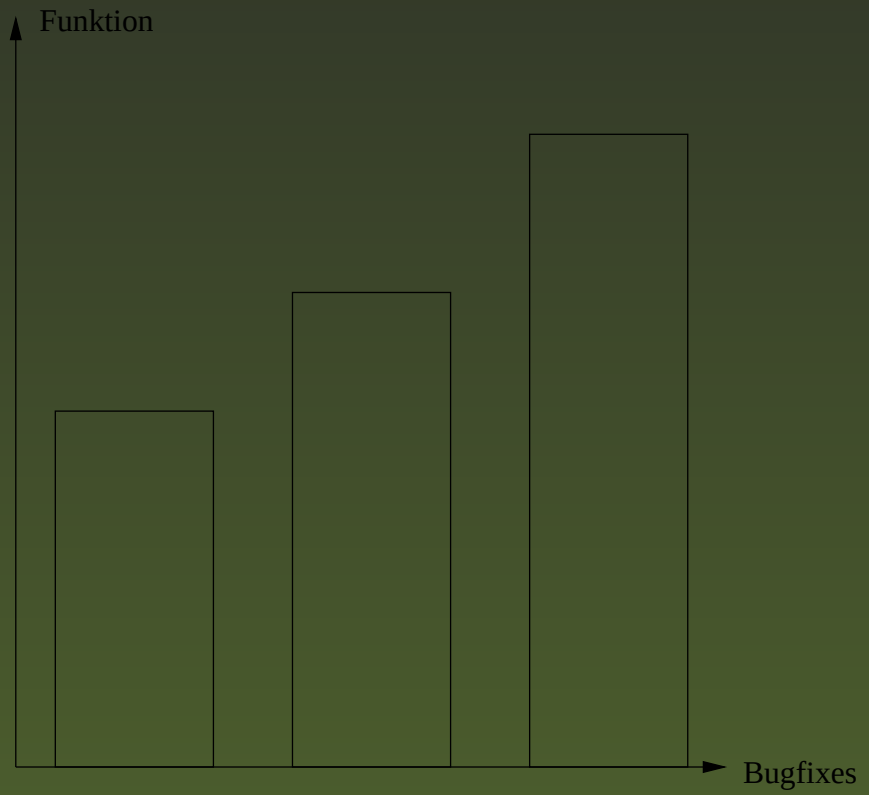
- Kann das alles stimmen?
- Zeitdifferenz zwischen zwei Radarimpulsen ist minimal
- Abweichung bei 0,0001%
- Passt nicht zur offiziellen Darstellung

Der Fehler – Die Wahrheit

- Software ist über dreissig Jahre alt
- Assembler Code
- Ungenauere Berechnungen
- Softwareupdates für Short Range Ballistic Missiles

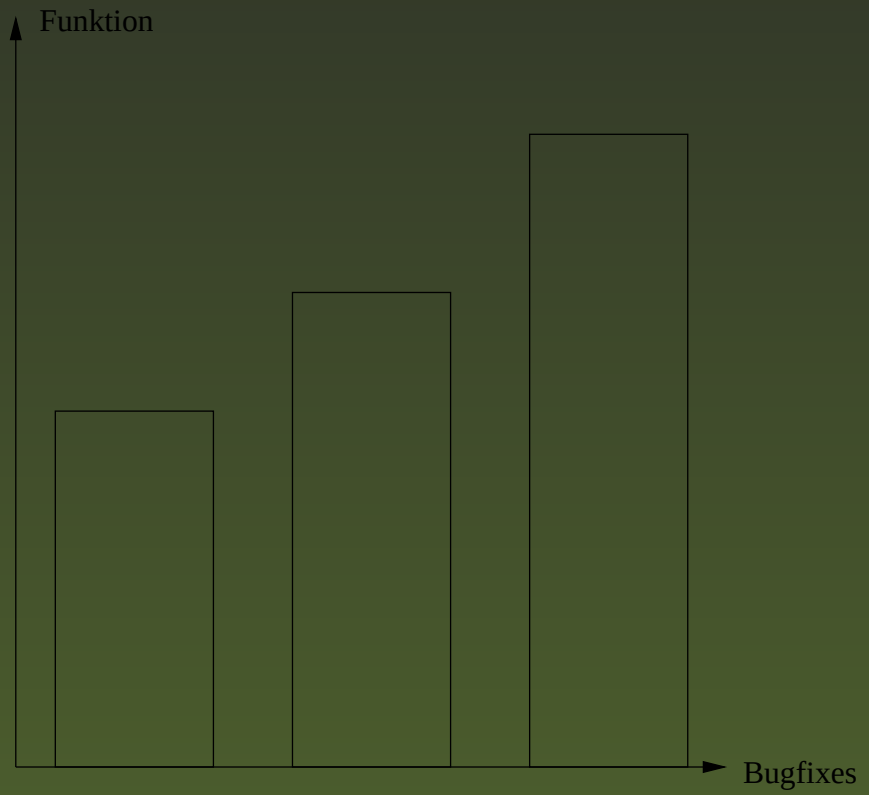
Der Fehler – Die Wahrheit

- Verbessern Bugfixes ein Programm?



Der Fehler – Die Wahrheit

- Verbessern Bugfixes ein Programm?



- Antwort: Leider nicht immer

Der Fehler – Die Wahrheit

- Subroutine zur genaueren Umrechnung der internen Uhr, durch ein Paar von 24-Bit Registern
- An etwa einem halben Dutzend Stellen eingebaut
- Dummerweise nicht an allen

Der Fehler – Die Wahrheit

- Aktuelle Zeit über alte Methode
- Tracken, Zielen und Berechnung des Abschusszeitpunktes über die akkuratere Methode.
- Akkurat berechnete Range Gate wurde zum falschen Zeitpunkt auf feindliche Objekte überprüft.

Verbesserungsvorschläge

- Mensch - Maschine?
- Warum wurden die Soldaten nur unzureichend informiert?
- Entwurfsmerkmale Mobilität und kurze Einsatzzeiten?
- Code-Fix schneller schicken?
- Rebooten?
  - Automatisch vs. manuell
  - Warnlichter

Verbesserungsvorschläge

- Bessere Spezifikation/Dokumentation?
- Höhere Modularität?
- High Level Programming Language? (1986)
- Bessere Verifikationsverfahren?
- Mehr Tests?

. . .und ihre Umsetzung?

Design der Siebziger sorgte für

- Numerische Schwachstellen
- Schlechte Wartbarkeit

. . .und ihre Umsetzung?

- Patriot nicht ausgereift
- Erster Einsatz gegen SCUDS
- Fehlendes Wissen, nur über Felderfahrung und Geheimdienste
- Keine Datenrekorder
- Zeitdruck, lieber schlecht als gar nichts?
- August 1990 - Februar 1991: Insgesamt sechs Patches

Weitere Fehlschläge

- Menschen wiegten sich in Sicherheit
- Patriots bis zu 10 Jahre aktiv
- Raketen hatten Probleme Steurungsinformationen zu empfangen (BBC News vom 24.März 2000)

Weitere Fehlschläge

Schuldfrage:

- Blindes Vertrauen?
- Fehlgeleitete/verlorengegange Informationen?

Weitere Fehlschläge

28.6.2003

- Tornado Kampfjet der British Royal Airforce abgeschossen
- Offiziell: Menschliches Versagen
- Inoffiziell: Raytheon Co.’s Automatikmodus

Weitere Fehlschläge

Fünf Tage zuvor:

- Pilot einer F-16 zerstört Patriotsystem

Patriot Einsatz Eignung

Ist das Patriot System überhaupt geeignet zu SCUD-Abwehr?

- Keinen Beweis für Funktionstüchtigkeit
- Keine wirklichen Dokumentationen
- 0-4 von 45 Raketen werden abgefangen
- Patriot ist langsamer als SCUD
- Erfolg bereits, falls Patriot den Pfad der SCUD kreuzte

Patriot Einsatz Eignung

Theodore Postol (MIT) und Reuven Pedatzur (Tel Aviv)

- Erfolgsrate unter 10% bzw. sogar 0%
- Nicht Sprengkopf, sondern Schwerpunkt ist Ziel
- SCUD-Flugbahn unvorhersagbar

Patriot Einsatz Eignung

- Erfolg war größtenteils psychologischer Natur
- Israelisches Verteidigungsministerium für Gegenschlag

Patriot Einsatz Eignung

Seit der Operation Desert Storm wurden 3 Milliarden US Dollar in das Patriot System investiert.

Patriot Einsatz Eignung

Dec 88 Production of the PATRIOT ATM Capability Two (PAC-2), a missile upgrade that increased the PATRIOT's kill capability to catastrophic kill, was authorized. - Red-stone