Therac-25

Seminar
Berühmt berüchtigte Softwarefehler

Bernhard Beckert

Referent:

Martin Pfeifer

Die Vorgänger

Therac-6

- Frühe 70er
- 6 MeV Beschleuniger
- Nur Röntgenstrahlung
- Besaß Computer, aber ohne wichtige Funktionen
- Hardware Interlocks als Sicherungssysteme

Die Vorgänger (II)

Therac-20

- Weiterentwicklung des Therac-6
- 20 MeV Beschleuniger
- Röntgen- und Elektronenstrahlung
- Computer hatte weiterreichende Aufgaben als bei Therac-6
- Sicherheitssysteme basierten auf Hardware

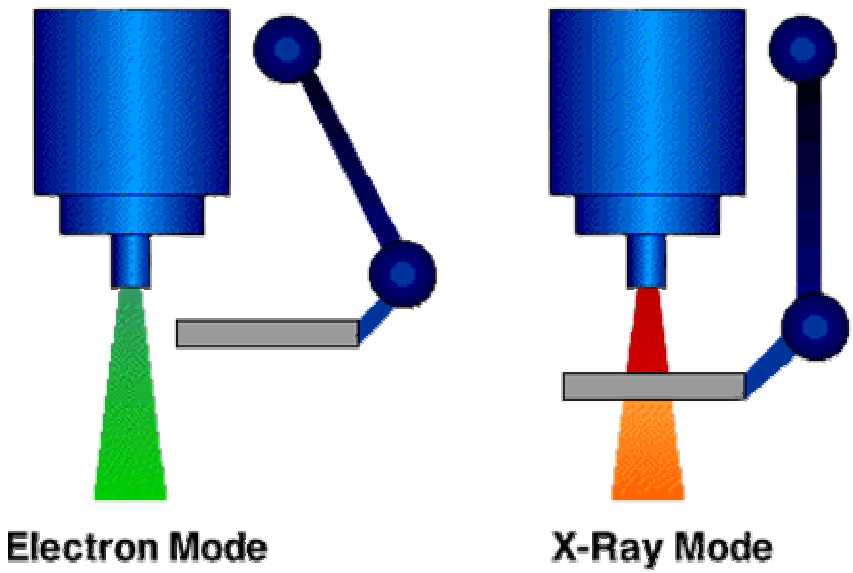
Thomson CGR und Atomic Energy of Canada Limited (AECL)

Das Gerät

Therac-25

- AECL
- Dualmode Linearbeschleuniger mit 25MeV Röntgenstrahlung oder variabler Elektronenstrahlung
- Kompakter und variabler als Vorgänger
- Größter Unterschied zu Vorgängern bestand in Benutzerführung
- Einstellung überwiegend an Konsole, nicht mehr am Gerät selber
- Sicherheitssysteme wurden durch Computer gesteuert

Das Gerät (II)



Das Gerät (III)

Um tiefer gelegene Tumore zu bestrahlen, musste Energie durch Bleiplatte gebündelt werden

Höhere Energie erforderlich

Fatal, wenn Platte bei Röntgenmodus nicht zwischen Gerät und Patient

So viel Strahlung wie nötig und so wenig wie möglich!

Ablauf einer Behandlung

Patient wurde auf dem Behandlungstisch platziert

Bestrahlungsfeld und Maschine wurden justiert

Techniker verließ den Raum

Techniker gab Patienten ID, Bestrahlungsfeld und Justierung ein

Nach der Eingabe wurden die Einstellungen zu „Verified“ und Behandlung konnte beginnen.

Display des Terminals

PATIENT NAME : TEST
TREATMENT MODE : FIX BEAM TYPE: X ENERGY (MeV): 25

	ACTUAL	PRESCRIBED	
UNIT RATE/MINUTE	0	200	
MONITOR UNITS	50 50	200	
TIME (MIN)	0.27	1.00	
GANTRY ROTATION (DEG)	0.0	0	VERIFIED
COLLIMATOR ROTATION (DEG)	359.2	359	VERIFIED
COLLIMATOR X (CM)	14.2	14.3	VERIFIED
COLLIMATOR Y (CM)	27.2	27.3	VERIFIED
WEDGE NUMBER	1	1	VERIFIED
ACCESSORY NUMBER	0	0	VERIFIED

DATE : 84-OCT-26 SYSTEM : BEAM READY OP. MODE : TREAT AUTO
TIME : 12:55: 8 TREAT : TREAT PAUSE X-RAY 173777
OPR ID : T25V02-R03 REASON : OPERATOR COMMAND:

Die Software

Kein kommerzielles Betriebssystem

Standalone realtime Betriebssystem

Computer war ein 32K PDP-11/23

Betriebssystem und Behandlungssoftware extra für Therac-25 in einer PDP-11 Assemblersprache geschrieben

Vier Hauptbestandteile:

- Gespeicherte Daten
- Scheduler
- Kritische und nicht kritische Tasks
- Interruptroutine

Die Fehlerbehandlung

Behandlungsunterbrechung auf zwei Weisen möglich:

- Treatment Suspend
  - Reset und Neustart des Systems
- Treatment Pause
  - System Pause, Fortsetzung der Behandlung durch Drücken der Taste P (Proceed)

Fehlermeldungen waren kryptisch und bestanden aus dem Wort *Malfunction* gefolgt von einer Zahl zwischen 1 bis 64

Gliederung

- Therac-25
- Die Unglücke
- Die Fehlfunktionen
- Reaktionen auf die Unglücke
- Weitere Fehler
- Fazit

Die Unglücke

Georgia, 03. Juni 1985

- Onkologisches Zentrum in Marietta
- 61jährige Frau mit Brusttumor
- Lähmungserscheinungen im Bereich der Schulter und des Armes, Brust musste entfernt werden
- Fehler wurde nie untersucht, AECL schloss Fehler ihrerseits aus

Die Unglücke (II)

Ontario, 26. Juli 1985

- Ontario Cancer Foundation Klinik in Hamilton
- 40jährige Frau mit Gebärmutterhalskrebs
- Nach fünf Sekunden stoppte System und gab H-tilt aus
- Gerät in Treatment Pause, Techniker drückte P
- Vorgang wiederholte sich vier Mal, dann Neustart

Die Unglücke (III)

Washington, 11. Dezember 1985

- Therac-25 im Yakima Krankenhaus wurde aufgrund des Vorfalls in Ontario mit Kontrollsoftware für Microswitch versehen
- Patientin mit Hautkrebs an der Hüfte
- Patientin überlebte, hatte aber seitdem eine steife Hüfte

Die Unglücke (IV)

Texas, 21. März 1986

- Tyler Klinik
- 33jähriger Patient mit Tumor im oberen Rücken
- Intercom defekt und Kamera ausgestöpselt
- Malfunction 54: Über- oder Unterdosis
- Beschädigung des Spinalkanals, später Lähmung der Beine

Die Unglücke (V)

Texas, 11. April 1986 Tyler Klinik

- 66jähriger Patient mit Hautkrebs im Gesicht
- Intercom wieder intakt
- Patient schrie auf, Technikerin sah nach
- Drei Wochen später verstarb er, Autopsie ergab, dass durch die Überdosis rechter Gehirnlappen und Stammhirn verletzt waren

Die Unglücke (VI)

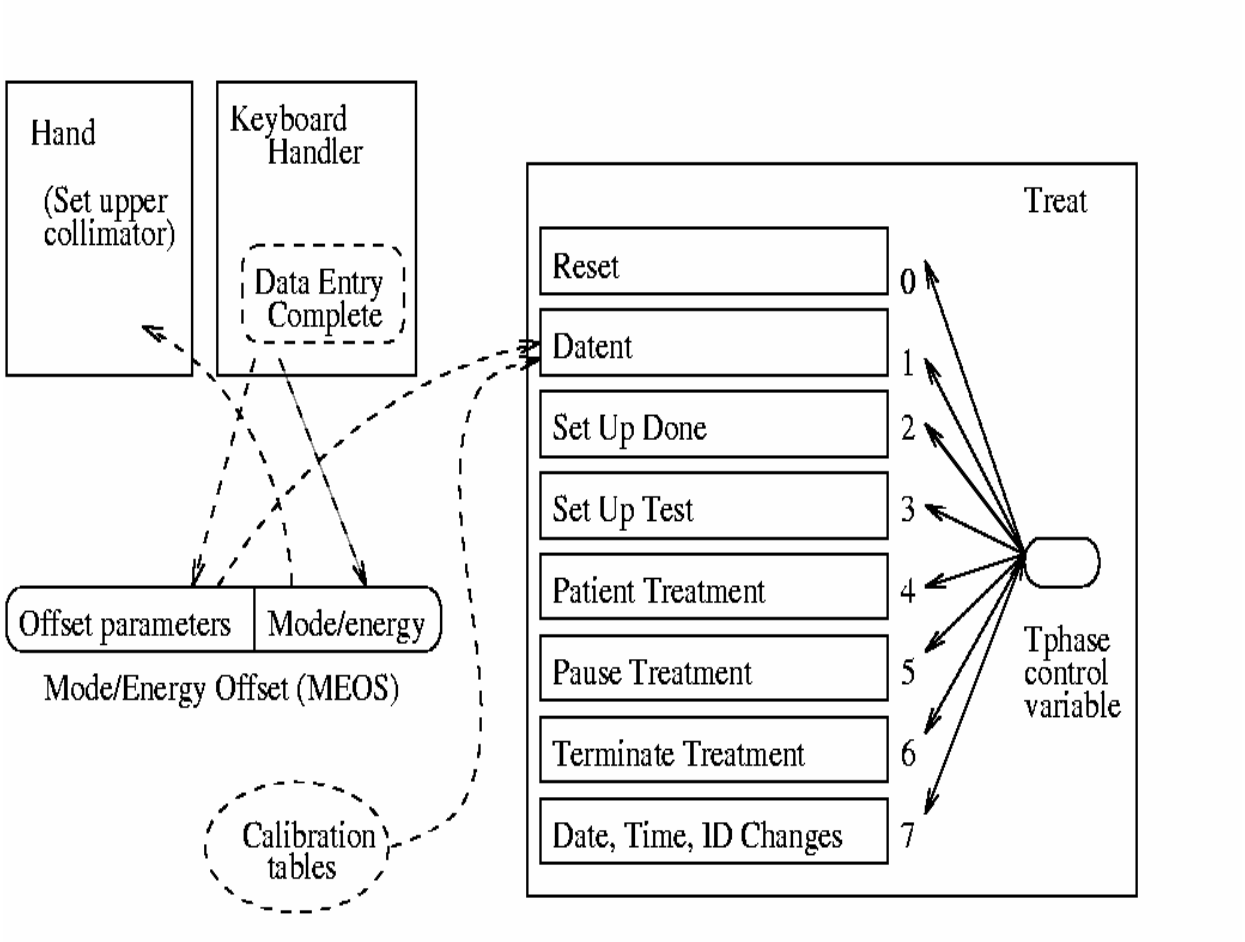
Washington, 17. Januar 1987

- Yakima Krankenhaus
- Elektronenstrahlenbehandlung war geplant, Patient erhielt Röntgenstrahlenbehandlung
- Patient verstarb im April

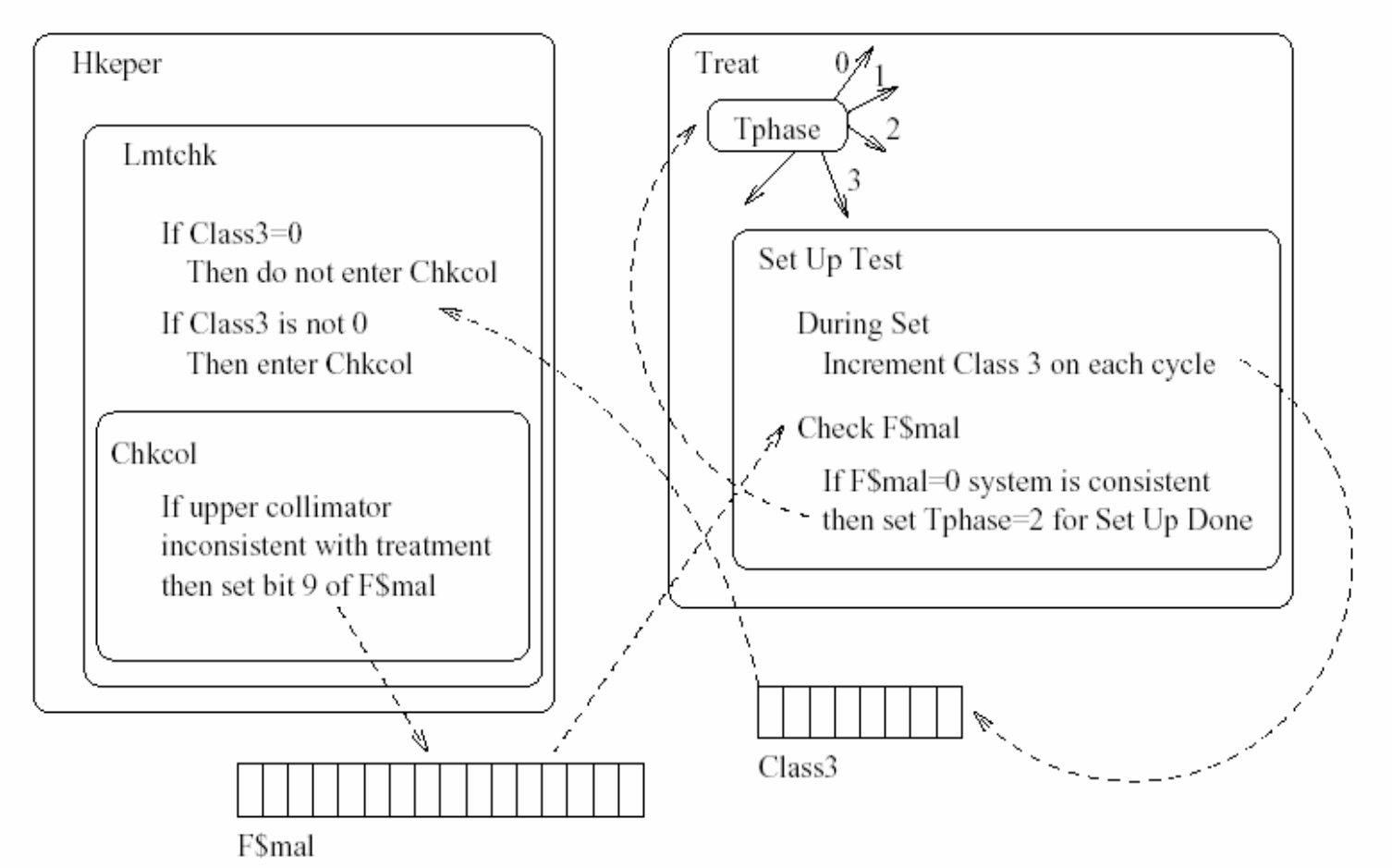
Gliederung

- Therac-25
- Die Unglücke
- Die Fehlfunktionen
- Reaktionen auf die Unglücke
- Weitere Fehler
- Fazit

Der Texas Bug



Der Washington Bug



Gliederung

- Therac-25
- Die Unglücke
- Die Fehlfunktionen
- Reaktionen auf die Unglücke
- Weitere Fehler
- Fazit

Reaktionen auf die Unglücke

2. Unfall Fehler konnte nicht reproduziert werden
   - Fehler wurde auf defekten Microswitch zurückgeführt

3. Unfall führte zu keiner Reaktion

4. Unfall AECL-Techniker stellte fest, Fehler lag nicht am System

Technikerin der Tyler-Klinik versuchte Fehler zu reproduzieren, FDA* wurde eingeschaltet und Texas-Bug wurde entfernt

---

*U.S. Food and Drug Administration, Department of Health and Human Services

Reaktionen auf die Unglücke (II)

Weiterer Unfall in Washington, weiterer Bug

- Therac-25 wurde runtergefahren
- Therac-25 wurde mit Hardware Interlocks ausgestattet und die Software wurde verbessert

Vermeidbarkeit

Zumindest einige Unglücke hätten verhindert werden können, wenn

- sofort nach dem ersten Unglück Untersuchungen erfolgt wären
- vor der Auslieferung bessere Tests durchgeführt worden wären
- der Umgang mit dem Gerät kritischer gewesen wäre
- nicht nur Software bei den Sicherheitssystemen verwendet worden wäre
- Fehlermeldungen selbst sprechend oder zumindest besser dokumentiert worden wären.

Gliederung

- Therac-25
- Die Unglücke
- Die Fehlfunktionen
- Reaktionen auf die Unglücke
- Weitere Fehler
- Fazit

Weitere Fehler

„Gleichzeitiges Auftreten eines Software-Fehlers mit einem Hardware-Ausfall bei Dosierung einer Arsen-Spritze. Der gesamte Inhalt führte zum Tod des Patienten“

Überwachungssystem für Intensiv-Patienten wurde vom Markt genommen, Software hat Daten den falschen Patienten zugeordnet

North Staffordshire Hospital Centre 1992
Programmierfehler, 10 Jahre lang 10-30 % zu geringen Strahlendosen bei insgesamt knapp 1000 Krebspatienten

Weitere Fehler (II)

Signale elektronischer Geräte, z.B. von Mobiltelefonen führen immer mehr zu Fehlfunktionen sensibeler medizinischer Geräte

Datenschutzverletzungen durch teilweise nicht vorhandenes Problembewusstsein einiger Ärzte im Umgang mit elektronischen Medien.

Tina Walber in ihrem Seminar „London Ambulance Dispatch“

Gliederung

- Therac-25
- Die Unglücke
- Die Fehlfunktionen
- Reaktionen auf die Unglücke
- Weitere Fehler
- Fazit

Fazit

Nicht nur auf einzelne Software-Bugs konzentrieren

Der explizite Fehler im Code nicht so wichtig wie Unsicherheit im Design von Software im Allgemeinen

Fehlermeldungen selbst sprechend oder zumindest hinreichend kommentiert

- Es traten bei dem Therac-25 über 40 Fehlermeldung pro Tag auf.

Nicht nur Symptome behandeln, sondern die Ursachen suchen und beheben

Fazit (II)

Zusätzliche Hardware-Sicherungen einbauen

Testen!

Umgang mit dem Therac-25 sehr unkritisch

Zielsetzung schon fragwürdig: Sicherheit vs. Bedienfreundlichkeit