Freie Universität Berlin

Vorlesung "Anwendungssysteme"

Sicherheit: Therac-25

Prof. Dr. Lutz Prechelt
Freie Universität Berlin, Institut für Informatik
http://www.inf.fu-berlin.de/inst/ag-se/

- Strahlentherapie und die Therac-Familie
- Die Unfälle
  - Exkurs: Der Drehkranz
- Softwareprobleme
  - "Cursor up"
  - Der Kollimatortest
- Ergriffene Maßnahmen
- Die Moral von der Geschicht'

Perspektive

Freie Universität Berlin

- Letzte Stunde:
  - Grundbegriffe von Sicherheit
  - Kurzbeispiele aus verschiedenen Bereichen
  - Grundbegriffe der Methodik für Sicherheit

- Heute:
  - Ausführliches Fallbeispiel
  - Betrachtung des Zusammenwirkens verschiedener Bereiche ("sozio-technisches System")
    - Technische Eigenarten und Probleme
    - Aktivitäten der Benutzer
    - Aktivitäten der Systemgestalter

AECL, CGR: Medizingeräte zur Strahlentherapie

- Die kanadische Firma Atomic Energy of Canada Limited (AECL) und die französische Firma CGR kooperierten seit den 1970er Jahren beim Bau von Linearbeschleunigern

- Eingesetzt zur Strahlentherapie, insbesondere bei Krebs
  - Elektronenstrahlen für oberflächliche Behandlung
  - Röntgenstrahlen für Behandlung tiefer liegenden Gewebes

AECL, CGR: Die Therac-Linie

Freie Universität Berlin

- Erstes Produkt: Therac-6
  - Ein 6 MeV-Beschleuniger, der Röntgenstrahlen abgibt
    - (ein normales Röntgengerät liefert 0,03 MeV bis 0,15 MeV)
  - basiert auf CGRs Neptune, plus ein DEC PDP 11 Steuercomputer (Software von CGR geschrieben)

- Zweites Produkt: Therac-20
  - Ein 20 MeV-Beschleuniger, der wahlweise Röntgen- oder Elektronstrahlung abgibt
  - basiert auf CGRs Saggitaire, plus ein DEC PDP 11

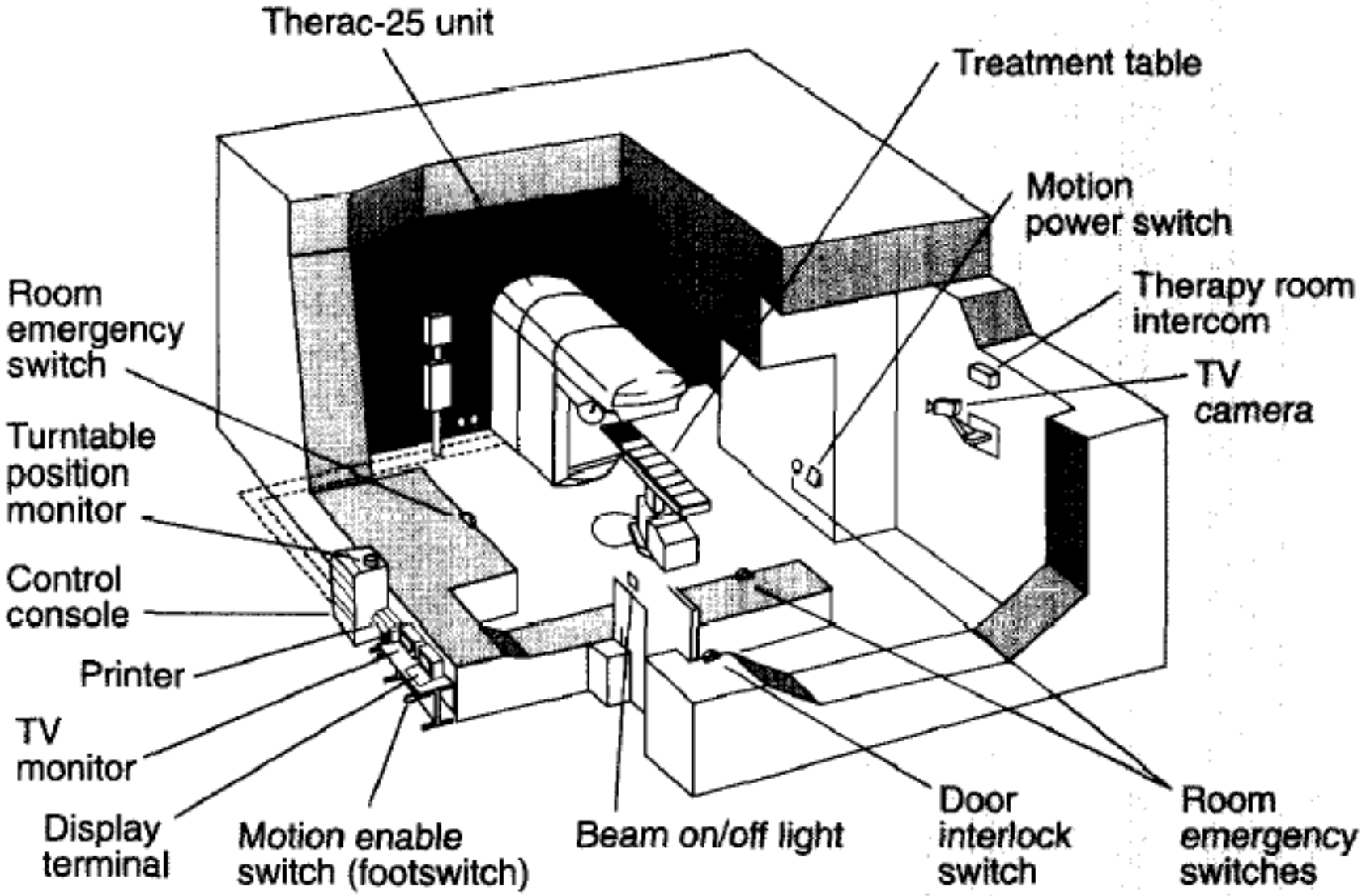
- Software ist nachträglich angebaut:
  - nur Komfortfunktionen, Betrieb auch ohne Computer möglich

AECL: Therac-25

Freie Universität Berlin

- Nach Therac-20 wurde die Zusammenarbeit von AECL und CGR aufgegeben
- AECL entwickelte ein viel besseres Beschleunigerprinzip
  - viel kompaktere Bauform und wesentlich preiswerter
- Drittes Produkt (nun ohne CGR): Therac-25 — Um den geht's!
  - Ein 25 MeV-Beschleuniger, der wahlweise Röntgen- oder Elektronstrahlung abgibt
    - Prototyp 1976, am Markt ab 1982
  - Von vornherein mit Computersteuerung entworfen
    - Insbesondere sind nun auch Sicherheitsfunktionen durch Software (statt HW) realisiert: Strahlüberwachung, Dosisbegrenzung
    - SW baut auf der von Therac-6 auf

Therac-25


Therac-25 unit
Treatment table
Motion power switch
Therapy room intercom
TV camera
Room emergency switch
Turntable position monitor
Control console
Printer
TV monitor
Display terminal
Motion enable switch (footswitch)
Beam on/off light
Door interlock switch
Room emergency switches

Die Unfälle mit Therac-25: Übersicht

Freie Universität Berlin

- Ab 1983 wurden 11 Therac-25-Maschinen installiert
- Zwischen 1985 und 1987 gab es 6 Unfälle mit massiven Überdosen von Strahlung
  - davon 2 mit tödlichem Ausgang
- 1987 wurde die Maschine vom Hersteller zurückgezogen und erheblich modifiziert
  - insbesondere wurden wieder Hardware-Sicherheitsmechanismen eingebaut
  - Dabei wurden auch gleichartige Softwaredefekte in Therac-20 entdeckt
    - die aber aufgrund dessen HW-Mechanismen nie zu Unfällen geführt hatten

Wir betrachten nun diese Unfälle, ihre Entstehung, die Abläufe drumherum und was man daraus lernen kann

Unfall 1: Marietta 1985

- Kennestone Regional Oncology Center in Marietta, Georgia
- 61-jährige Patientin, Nachbehandlung nach Entfernung eines bösartigen Tumors in der Brust
  - 10 MeV Elektronenbehandlung
  - Patientin fühlt rotglühende Hitze, sagt "Sie haben mich verbrannt"
  - Techniker: "Das ist unmöglich"
- Krankenhaus-Physiker fragt bei AECL, ob Therac-25 theoretisch eine Elektronenbehandlung ohne Strahlauffächerung (scanning) machen könnte
  - Antwort von AECL nach 3 Tagen: Nein, unmöglich.
- Patientin verklagt Krankenhaus, AECL und die Wartungsfirma

Unfall 1: Marietta 1985 (2)

Freie Universität Berlin

- AECL unternimmt keine Nachforschungen
  - Kein entsprechender Geschäftsprozess ist installiert
- Patientin entwickelt starke Rötung und Schwellung in der Behandlungszone
  - starke Schmerzen, Krämpfe
  - Rötung am Rücken an der gleichen Stelle
- Strahlenbehandlung wird dennoch zunächst normal fortgesetzt

Beispiel: Verbrennungen durch Strahlung

Freie Universität Berlin

Exkurs: Strahlungsdosis

Freie Universität Berlin

- Physik:
  - Strahlungsdosis ist die eingestrahlte Energiemenge *pro Masseneinheit*: Joule pro Kilogramm
    - genannt "**absorbierte Dosis**"
  - Die SI-Einheit heißt gray (gy): **1 gray = 1 J/kg**
  - Alte Einheit hieß rad: 1 gray = 100 rad

- Biologie:
  - Für die biologische Wirkung kommt es darauf an, wie viele und welche Teile des Körpers eine Strahlungsdosis empfangen und welche Art von Strahlung es ist

Strahlungsempfindlichkeit: Faustregeln

Freie Universität Berlin

Bei Bestrahlung des gesamten Körpers
(mit harter Röntgen- oder Gammastrahlung)

- 1 gray: Milde Strahlenkrankheit: Kopfschmerz, Störung des Immunsystems
- 2 gray: Leichte Strahlenvergiftung: 10% Todesfälle binnen 30 Tagen; Erbrechen; Sterilität bei Männern
- 5 gray: Akute Strahlenvergiftung: 50% Todesfälle; Blutungen im Mund, unter der Haut, in den Nieren.
  - Die Überlebenden entwickeln später in der Regel Krebs
- 50 gray: Koma binnen Minuten; Tod binnen Stunden

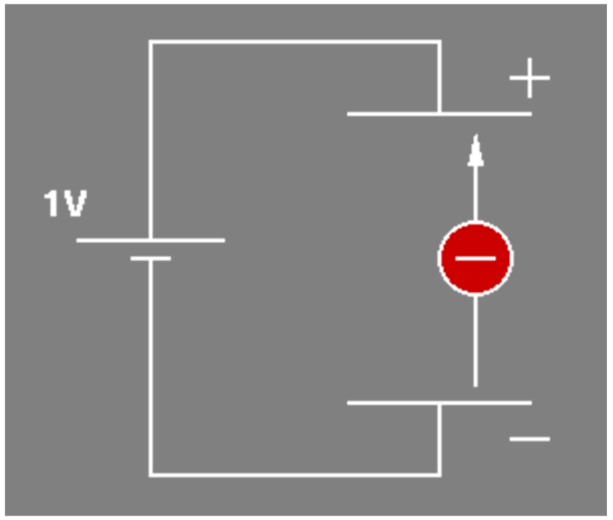
In der Strahlentherapie:

- Typische Behandlungsdosen sind ca. 2 gray
  - manchmal auch einiges mehr oder weniger
  - aber *angewendet nur auf kleine Körperregionen*

Exkurs:
Parameter für Therac-Strahlungsdosis

Freie Universität Berlin

- Die Leistung des Beschleunigers (25 MeV) beschreibt die Energie eines einzelnen Elektrons
  - Wichtig für die Wirktiefe im Gewebe
  - Therac produziert Elektronen stoßweise



- Weitere Parameter für die Gesamtdosis:
  - Wie viele Elektronen hat ein Puls?
    Wie viele Pulse gibt es pro Sekunde?
  - Wie lange dauert die Behandlung insgesamt?
  - Wie viel wird von der Strahlfeldbegrenzung abgefangen?
  - Bei Röntgenbehandlung: Wie viel geht durch die Wandlung in Photonen verloren?

Unfall 1: Marietta 1985 (3)

(Fortsetzung:)

- Geschätzte Dosis: 150–200 gray (ein oder zwei Mal)

- Folgen:
  - Brust musste wegen der Verbrennungen entfernt werden
  - Lähmung von Schulter und Arm

- Es gab lange keine Meldung des Unfalls an die FDA
  - Food and Drug Administration: US-Arzneimittelbehörde
  - Gesetzeslage: Hersteller mussten schwere Unfälle melden; Anwender (Krankenhäuser) jedoch nicht

Unfall 2: Hamilton 1985

Freie Universität Berlin

- Ontario Cancer Foundation in Hamilton, Ontario
  - 7 Wochen nach dem ersten Unfall
  - Therac-25 ist hier schon 6 Monate in Betrieb
- 40-jährige Patientin mit Gebärmutterhalskrebs
  - 24. Termin der Strahlenbehandlung

- Maschine gestartet; stoppt nach 5 Sekunden;
  Meldung "H-tilt";
  Anzeige besagt "Dosis null, Behandlungspause"
  - Bediener drückt "P" (proceed) zum Fortsetzen
  - Das war Standardverfahren, da ungefährliche Fehlfunktionen häufig auftraten
- Es gab insgesamt 5 Durchläufe direkt hintereinander mit diesem Verhalten

Unfall 2: Hamilton 1985 (2)

Freie Universität Berlin

- Dann zeigte die Maschine "Behandlungsabbruch"
- Techniker wurde gerufen, fand aber kein Problem
  - Auch dies war ein nicht ungewöhnliches Ereignis
- Patientin klagte über "elektrisches Prickeln" in der Behandlungszone
  - Andere Patienten wurden am gleichen Tag ohne Probleme behandelt
- Bei nächster Behandlung, 3 Tage später, klagt Patientin über Brennen, Hüftschmerzen und starke Schwellung der Behandlungszone
  - Maschine wird außer Betrieb genommen:
    Verdacht auf Strahlen-Überdosis

Unfall 2: Hamilton 1985 (3)

Freie Universität Berlin

- Meldung an AECL
- Patientin starb 3 Monate später an extrem virulentem Krebs
  - Obduktion ergab ferner:
    Zerstörung der Hüfte durch die Strahlendosis
- Geschätzte Dosis: 130-170 gray

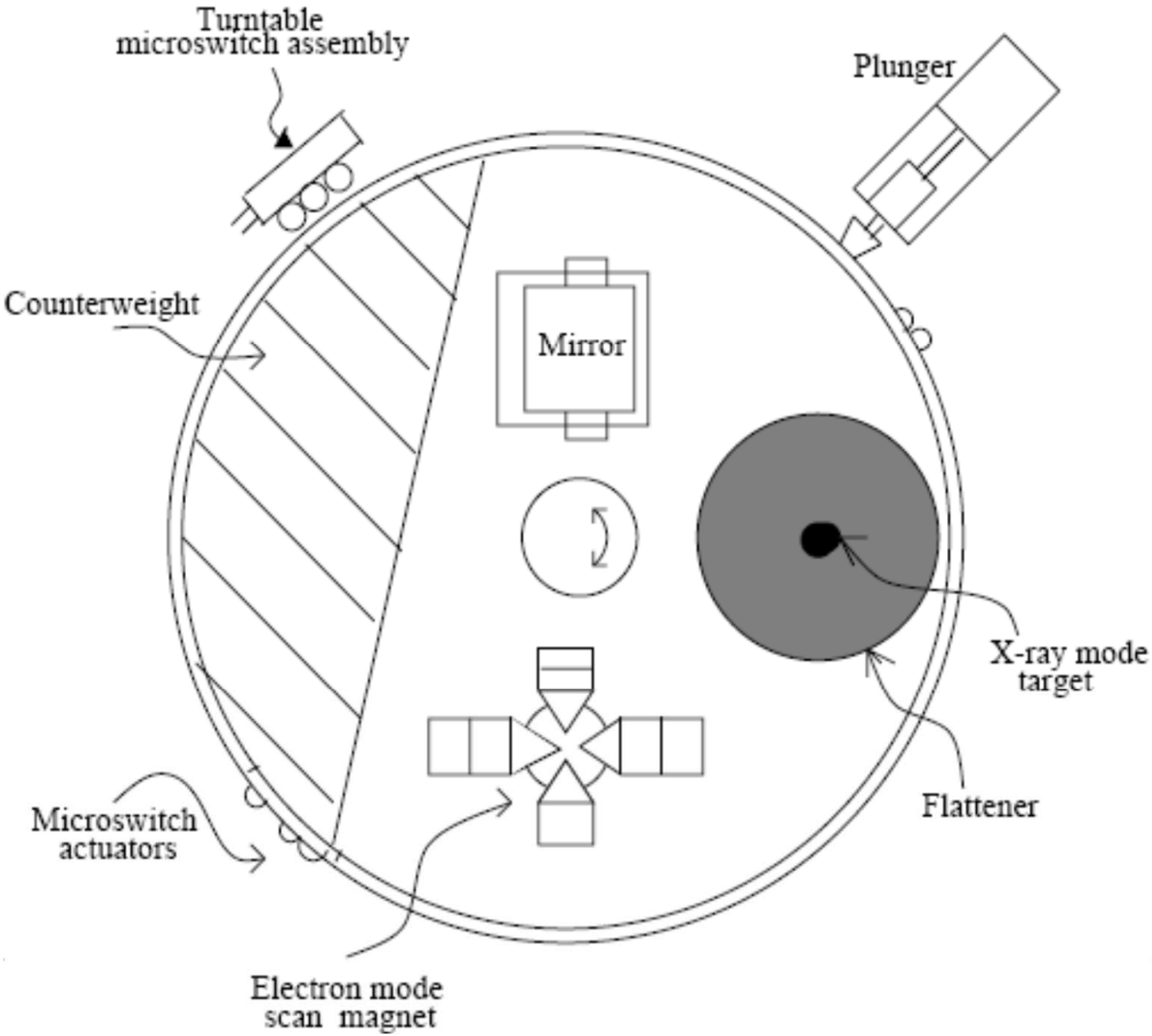
Unfall 2: Erkenntnisse von AECL

Freie Universität Berlin

- AECL konnte das Versagen nicht reproduzieren

- Sie vermuteten ein transientes Versagen eines Mikroschalters, der die Position des Drehkranzes prüft
  - zusammen mit einem anderen Problem im mechanischen Aufbau der Drehkranz-Steuerung
  - Sie modifizierten die Steuerungssoftware, um solche Fehler tolerieren zu können
  - Und behaupteten hinterher eine Verbesserung der Sicherheit gegenüber Schalterversagen um Faktor 100.000

Exkurs 1:
Der Drehkranz von Therac-25



Exkurs 1:
Der Drehkranz von Therac-25 (2)

Freie Universität Berlin

3 Stellungen für 3 Betriebsmodi

- Patienten positionieren (Beleuchtungsstellung):
  - Im Strahlgang ist ein Spiegel, der einen Lichtstrahl dorthin lenkt, wo der Behandlungsstrahl sein wird
- Elektronenstrahl-Behandlung:
  - Im Strahlgang liegen Magneten, die per Wechselfeld den konzentrierten Elektronenstrahl auffächern, sowie ein Messgerät für Strahlintensität
- Röntgen-Behandlung:
  - Im Strahlgang liegen ein Diffusor, der den sehr intensiven Elektronenstrahl in Röntgenstrahlung wandelt, stark abschwächt und verbreitert, sowie ein Messgerät
    - Die Röntgenstrahlung wird aus dem Elektronenstrahl erzeugt, der dafür ca. **100 mal so stark** ist, wie bei Elektronstrahl-Behandlung

Exkurs 1: Drehkranz, Konsequenzen

Freie Universität Berlin

- Diese Konstruktion bedeutet, dass:
  - wenn der Computer "glaubt", der Drehkranz sei in Stellung "Röntgenbehandlung",
  - in Wirklichkeit jedoch der Drehkranz in Stellung "Patientenpositionierung" ist,

- dann die 100-fach überhöhte Elektronstrahlung auf den Patienten wirkt
  - und zugleich als Dosis 0 gemessen wird, weil das Messgerät gar nicht im Strahlengang ist.

Exkurs 2: Benutzungsschnittstelle (geplant)

Freie Universität Berlin

Die Bedienung von Therac-25 war wie folgt entworfen:

- Bediener arrangiert Patienten auf dem Behandlungstisch,
- stellt das Bestrahlungsfeld ein und installiert ggf. nötiges Zubehör.
- Bediener geht dann aus dem Behandlungsraum an die Konsole (ein DEC VT 100 Bildschirmterminal)
  - und gibt dort alle diese Einstellungen nochmals ein
  - sowie Patientenkennung und Bestrahlungsbeschreibung (Modus, Energie, Dosis, Dosisrate oder Zeit)

Exkurs 2: Benutzungsschnittstelle (gebaut)

Freie Universität Berlin

- Testbenutzer des Prototyps beklagten, dieses Verfahren sei zu umständlich

- Die Software wurde deshalb modifiziert:
  - Anstelle einer *Eingabe* der Geräteeinstellungen aus dem Behandlungsraum konnten diese durch Tippen von RETURN automatisch von den Gerätesensoren übernommen werden

  - Es sinkt dadurch die Chance, dass das Problem aufgedeckt wird, falls die Sensoren einmal "irren"

Exkurs 2: Benutzungsschnittstelle (3)

Freie Universität Berlin

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:

Exkurs 3: Fehlerbehandlung der Therac-25 SW

Freie Universität Berlin

- Stellte die Software einen Fehlerzustand fest, wurde die Behandlung abgebrochen

- 2 Arten:
  - "Behandlungspause": Konnte mit Eingabe "P" (proceed) fortgesetzt werden
  - "Behandlungsunterbrechung": Nach fünf Fehlern. Verlangt ein komplettes Rücksetzen und Neueingabe aller Parameter

- Fehlermeldungen:
  - waren kryptisch
  - meist von der Art "malfunction 1" bis "malfunction 64"
  - Die Dokumentation enthält anfangs keine Erläuterung dieser Meldungen
  - und sagt auch nicht, wann Patientengefährdung möglich ist

Unfall 2: Ergriffene Maßnahmen

Freie Universität Berlin

- AECL meldet an FDA und CRPB
  - Diese überwachen die Maßnahmen von AECL
  - CRPB verlangt den Einbau eines zweiten, unabhängigen Messsystems (Potentiometer) für die Drehkranzposition
  - CRPB verlangt, dass die Aktion "p" (proceed) bei unerwarteter Dosisanzeige unmöglich sein soll

- Maßnahmen von AECL:
  - Meldung an Therac-25-Anwender:
    "Es gibt ein Problem. Überprüft stets die Drehkranzposition optisch."
  - Die Schranke für "p"-Aktionen wird von 5 mal hintereinander auf 3 mal gesenkt
  - Ein Potentiometer wurde nicht nachgerüstet

Unfall 3: Yakima 1985

- Yakima Valley Memorial Hospital in Yakima, Washington
  - 3 Monate nach der Modifikation nach Unfall 2
- Patientin entwickelt starke Hautrötung mit Streifenmuster im Behandlungsbereich (Hüfte)
  - Behandlung wird mehrere Wochen bis zu Ende fortgesetzt
  - da die Rötung als nicht gefährlich eingestuft wird
- Das Krankenhaus sucht aber intensiv die Ursache
  - und röntgt sogar die Heizdecke der Frau aus deren heimischem Bett, weil deren Heizdrähte als Ursache vermutet waren
  - findet aber keine Begründung

Unfall 3: Yakima 1985 (2)

Freie Universität Berlin

- Krankenhaus fragt bei AECL an (telefonisch, brieflich)
- Antwort von AECL:
  - "Wir glauben, dass es nicht durch Fehlfunktion oder Bedienerfehler am Therac-25 entstanden sein kann."
  - Antwort enthält diverse Begründungen, einschließlich: "Es hat offenbar keine anderen solchen Fälle gegeben."
- Die Patientin entwickelte Monate später Hautgeschwüre und Nekrose (absterbendes Gewebe) an der Stelle
  - Konnte beides behoben werden
  - Außer Vernarbung wenig bleibende Schäden

Unfall 4: Tyler 1986

Freie Universität Berlin

- East Texas Cancer Center in Tyler, Texas
  - Maschine schon 2 Jahre in Betrieb, 500 Patienten behandelt
- Männlicher Patient
  - 9. Nachbehandlung nach Entfernung eines Rückentumors
  - Geplant: Elektronenbehandlung 22 MeV, 1.8 gray auf ein Feld von 10x17cm am Rücken
    - insgesamt 60 gray verteilt über 6 Wochen
- Bedienerin war sehr erfahren und schnell mit Therac-25
  - Sie gab versehentlich "Röntgen" statt "Elektronenstrahl" ein, merkte dies aber vor dem Start und korrigierte die Eingabe mit den Cursortasten
    - Der Rest der Parameter blieb stehen
  - Maschine stoppte sofort nach Start mit Meldung "*malfunction 54*" und "Behandlungspause"

Unfall 4: Tyler 1986 (2)

Freie Universität Berlin

- Das an der Konsole befestigte Merkblatt erklärte diese Meldung mit "*dose input 2 error*"
- Genauere Information lag auch im Handbuch nirgends vor
  - AECL erklärte viel später, die Meldung könne Überdosis oder Unterdosis anzeigen
- Konsole zeigte starke Unterdosis an
  - 6 Einheiten anstatt 202 verlangten Einheiten

- Bedienerin drückte wie üblich "p"
  - Maschine stoppte sofort nach Start erneut mit Meldung "*malfunction 54*" und "Behandlungspause"

- Der Patient erhielt eine Überdosis und spürte dies
  - Er empfand es wie einen elektrischen Schock oder als wenn jemand "Kaffee über seinen Rücken geschüttet" hätte
    - er wusste, dass dies nicht normal war (es war ja die 9. Behandlung)

Unfall 4: Tyler 1986 (3)

- An diesem Tag war der Videomonitor zur Kamera des Behandlungsraums nicht angeschlossen und die Sprechanlage defekt
  - Der Patient sprang vom Behandlungstisch auf und hämmerte gegen die Tür
  - Beim Aufstehen traf ihn die zweite Behandlung
  - Bedienerin öffnete bestürzt die Tür

- Patient wurde sofort untersucht:
  - Hautrötung, eingestuft als Folge eines Elektroschocks
  - Nach Hause geschickt: "Kommen Sie wieder, falls weitere Folgen auftreten."

Unfall 4: Tyler 1986 (4)

Freie Universität Berlin

- Der Physiker des Krankenhauses untersuchte Therac-25
  - Fand alle Kalibrierungen und Funktionen intakt
  - Weitere Behandlungen des Tages wurden durchgeführt
- Der Patient hatte tatsächlich eine enorme Dosis erhalten
  - 16-25 gray binnen 1 Sekunde auf 1x1cm Fläche
- Er entwickelte zahlreiche Schäden
  - Schmerzen im Nacken und am Arm, Erbrechen und Schwindel, strahlungsbedingte Paralyse des linken Arms und beider Beine, Fehlfunktionen von Darm und Blase, Lesion der linken Lunge, Paralyse des linken Zwerchfells
- und starb nach 5 Monaten an den Folgen

Unfall 4: Ergriffene Maßnahmen

Freie Universität Berlin

- AECL schickte am Tag nach dem Vorfall zwei Testingenieure
  - Testeten einen Tag lang die Maschine
  - Konnten die "*malfunction 54*" nicht reproduzieren
  - Einer erklärte auf Befragen, dass keine anderen Vorfälle mit Überdosis bekannt seien
  - Vermutung: Unfall entstand durch "ein elektrisches Problem"
- Eine unabhängige Firma prüfte die Erklärung
  - Sie befand die Maschine für korrekt geerdet und elektrischen Schocks unverdächtig
- Maschine ging wieder in Betrieb

Unfall 5: Tyler 1986

Freie Universität Berlin

- Wieder im gleichen Krankenhaus
  - drei Wochen nach dem ersten Unfall

- Gleiche Bedienerin:
  - Geplante Behandlung: 10 MeV Elektronenstrahl auf eine Fläche von 7x10 cm
  - Bedienerin gab wieder erst versehentlich "Röntgen" statt "Elektronenstrahl" ein, merkte dies wieder vor dem Start und korrigierte wieder die Eingabe mit den Cursortasten
  - Maschine stoppte kurz nach Start mit Meldung "*malfunction 54*" und "Behandlungspause"
  - Bedienerin hörte über die Sprechanlage erst ein lautes Geräusch, dann lautes Klagen des Patienten

Unfall 5: Tyler 1986 (2)

- Wahrnehmungen des Patienten
  - "Etwas hat mich an der Seite des Gesichts getroffen, ich sah einen Lichtblitz und hörte ein brutzelndes Geräusch wie beim Spiegelei-Braten."

- Der Patient entwickelte hohes Fieber, Desorientierung, neurologische Schäden und schließlich Koma

- Er starb drei Wochen nach dem Unfall
  - Die Autopsie ergab schwere Strahlungsschäden im rechten Hirnlappen und im Hirnstamm

Unfall 5: Ergriffene Maßnahmen

Freie Universität Berlin

- Die Maschine wurde sofort außer Betrieb genommen
- Der Physiker des Krankenhauses und die Bedienerin begannen eine genaue Untersuchung
  - Nach langer Mühe gelang es den beiden, "*malfunction 54*" zu reproduzieren
  - Die Überdosis geschah dann, wenn die Geschwindigkeit der Dateneingabe an der Konsole sehr hoch war
  - Nach einiger Übung gelang die Reproduktion nach Belieben
  - Nun maß der Physiker die Strahlungsdosis: ca. 40 gray

Unfall 5: Ergriffene Maßnahmen (2)

Freie Universität Berlin

- AECL konnte das zunächst nicht reproduzieren
  - Erst nach genauer Anleitung gelang es ihnen auch
  - Sie maßen dann 250 gray
  - Behandlungsdauer war 0,3 Sekunden, mit enorm verschiedenen Dosen auf verschiedenen Maschinen
  - Genaue Dosis ist deshalb unbekannt
- Ein AECL-Ingenieur sagte später in einem Gerichtsverfahren aus, es habe ein Jahr zuvor in zwei Kliniken ein "cursor up"-Problem gegeben
  - und die Software sei korrigiert worden.
  - Es ist nicht sicher, dass es sich um das selbe Problem handelt

Die Entwicklung der Therac-25-SW

Freie Universität Berlin

- Aus der Therac-6-SW (begonnen 1972) entwickelt
  - Übernahme ca. 1976
- von 1 Person über mehrere Jahre in PDP-11 Assembler
  - Über Ausbildung und Erfahrung dieser Person ist nichts bekannt
    - trotz Untersuchung vor Gericht!
- Wenig Dokumentation verfügbar:
  - Keine Spezifikationen, kein Testplan
- AECL:
  - "HW und SW wurden einzeln und gemeinsam über viele Jahre hinweg getestet" (ca. 2700 "Benutzungsstunden")
  - "Ein geringer Teil der Tests basierte auf einem Simulator, das meiste jedoch erfolgte im Gesamtsystem"
- Offenbar wurden kaum Modultests durchgeführt

Architektur der SW

- Läuft ab auf PDP-11/23 (16 bit, 3.4 MHz, 32 KB RAM)
- Selbstgeschriebenes Echtzeit-Betriebssystem
  - kein Standard-Betriebssystem benutzt
- Präemptives Steuerprogramm (*scheduler*)
  - d.h. echter Mehrprogrammbetrieb (*multitasking*)
  - Unterscheidung in kritische und nichtkritische Aufgaben
- Wichtigste andere Teile der Software:
  - Unterbrechungsdienste (*interrupt services*)
  - Routinen für kritische/nichtkritische Aufgaben
  - gemeinsame Daten
- Inhalt der gemeinsamen Daten:
  - Kalibrierungsparameter der Maschine
  - Parameter der aktuellen Behandlung

Architektur und Defekte

Freie Universität Berlin

- Im Detail sind der Entwurf und die Kodierung der SW extrem verworren

- Das ist die Grundlage für die zwei schweren Defekte, die die Unfälle ermöglicht haben
  - Das "Cursor-up"-Problem
  - Das Kollimatortest-Problem

- Siehe nächste Folien

Das "Cursor up"-Problem: Quelle und Wirkung

Freie Universität Berlin

- Nach Beendung der Eingabe werden die Parameter der Maschine eingestellt
  - Dauert 8 Sekunden
- Durch schlechten Entwurf plus einen Programmierfehler ergibt sich folgendes Verhalten:
  - Wird vor Ablauf der 8 Sekunden eine Parameteränderung begonnen *und abgeschlossen*, merkt die Haupt-Eingabeverarbeitungs-Routine die Änderung der gewählten Energie nicht
    - Cursor scheint die "fertig"-Position nie verlassen zu haben
  - Die Umstellung der Betriebsart (Elektronen ⇔ Röntgen) wird jedoch von einer ganz anderen nebenläufigen Routine behandelt und korrekt durchgeführt
    - Eine Konsistenz-Überprüfung gibt es nicht.

Das Kollimatortest-Problem

Freie Universität Berlin

- Eine andere periodisch ablaufende Routine prüft, ob die Einstellung des Kollimators für die aktuellen Behandlungsparameter zulässig ist

- Sie setzt bei "unzulässig" die Anzeigevariable falsch:
  - anstatt `unsicher = 1`
  - macht sie (aus Speicherplatzgründen) `unsicher++`

- Dadurch läuft diese 8-bit-Variable periodisch über:
  - $255+1 = 0 \pmod{2^8}$

- Falls zufällig genau in dem Moment die Behandlung gestartet wird, wird eine ggf. falsche Einstellung nicht abgewiesen.

Zwischenbilanz

Erkenntnisse bis hierher:

1. Trotz großer Sicherheitsanstrengungen sind Unfälle passiert
   - dafür brauchte man zusätzlich Pech,
     wie z.B. die tüchtige Bedienerin
   - aber früher oder später hat man halt immer mal Pech
2. Die Ursachen der Unfälle waren schwer aufzuklären,
   - weil schon die Reproduktion der Umstände schwierig war
   - was daran lag, dass Zeitbedingungen im Spiel waren
3. Ganz zuunterst lagen Programmierfehler
   - aber die sollte man nicht zur Ursache erklären:
4. das eigentliche Hauptproblem war der Verzicht auf software-unabhängige Sperrschaltungen

Prozesschaos

- Neben diesem Produktproblem gab es aber vor allem Prozessprobleme:
  - Unzureichende Geschäftsprozesse (s. oben)
  - Geringe Handlungsbereitschaft
  - Nachbesserungs-Mentalität

- Schauen wir uns das mal an:

Aktionen von AECL

- Nach ihrer Untersuchung der Tyler-Unfälle und der Diagnose (aber nicht Lösung) des "cursor up"-Problems sendete AECL folgenden Brief an die Therac-25-Anwender [übersetzt und verkürzt wiedergegeben]:
  - "Betreff: Änderung der Betriebsverfahren für Therac-25.
    Die Taste "*cursor up*" darf ab sofort nicht mehr zum Ändern der Behandlungsdaten verwendet werden.
    Um versehentliche Benutzung zu verhindern, entfernen Sie die Tastenkappe und fixieren Sie den Tastenkontakt mit Isolierband in Stellung "offen".
    Sprechen Sie zur Unterstützung dafür Ihren örtlichen AECL-Techniker an.
    Bei irgendwelchen Eingabefehlern muss deshalb nun "R" (reset) benutzt und die gesamte Eingabe wiederholt werden."

Aktionen der FDA

- FDA widersprach dem Brief:
  - "Beschreibung des Problems und der Begründung fehlen.
    Dringlichkeit nicht genügend klar."

- FDA verlangte von AECL einen "corrective action plan" (CAP, Aktionsplan über Behebungsmaßnahmen)
  - muss bei FDA vorgelegt und freigegeben werden

- AECL bat zunächst um Aufschub,
  reichte später einen Plan mit 6 Maßnahmen ein
  - dieser wurde von FDA ausführlich kommentiert und als unzureichend abgelehnt

Weiterer Verlauf

Freie Universität Berlin

- Eine Therac-Benutzergruppe gründete sich
  - versuchte, selbst entworfene Verbesserungen bei AECL unterzubringen
- FDA erzwang 4 Nachbesserungen des Plans:
  - Version 2, Version 3, Version 4, Version 5
  - Unterwegs großes Hin und Her und Mängel bei Nachbesserungen von AECL:
    - FDA-Memo nach Version 4: "Die Tabellen im Testprotokoll, die das Funktionieren der Korrektur nachweisen sollen, zeigen das genaue Gegenteil:
      Die eingegebenen Werte für Strahltyp und Energie nach dem Editieren verändern nicht wirksam die vorherigen Einstellungen.
      Entweder ist die Korrektur falsch oder das Protokoll ist unzutreffend."
- Vor Version 3 kam es in Yakima zu noch einem Unfall

Unfall 6: Yakima 1987

- Bediener startet die Therapie
  - Maschine schaltet Strahl ein, zeigt aber Dosis Null
  - pausiert nach 5 Sekunden mit einer Meldung
    - Meldung konnte nicht rekonstruiert werden
  - Bediener setzt mit "p" fort
  - Erneute Pause, Meldung "flatness"
- Patient klagt über "brennendes Gefühl in der Brust"
  - Konsole zeigt als Dosis 0,07 gray
  - Patient entwickelt erst Rötung, später Streifenmuster
  - Stirbt nach 3 Monaten an Komplikationen der Überdosis
- Untersuchung des Unfalls ergibt:
  - Der Elektronenstrahl wurde eingeschaltet, obwohl der Drehkranz in Beleuchtungsstellung war
  - Dosis ca. 80–100 gray

Aktionsplan Version 5

Freie Universität Berlin

- AECL legte nach insgesamt 14 Monaten die später auch umgesetzte Fassung 5 des Plans vor. Inhalt:
  - Alle Dosen-bezogenen Unterbrechungen führen zu Neustart und verlangen Neueingabe aller Parameter (kein "p" mehr)
  - Eine Abschaltung nach hohen Einzelpulsen wird in Software realisiert
  - Eine davon unabhängige Abschaltung nach hohen Einzelpulsen wird in Hardware realisiert
  - Die Überwachungslogik für den Drehkranz wird verbessert, um sicher erkennen zu können, wenn er sich nicht in einer gültigen Position befindet.
  - Ein Drehkranz-Potentiometer wird ergänzt, sowie eine optische Anzeige der Drehkranz-Position für den Bediener
  - Strahleinschaltung wird verhindert, wenn der Drehkranz in Beleuchtungsstellung oder einer Zwischenstellung ist

Aktionsplan Version 5 (2)

- Eine Kopplung von Röntgenmodus und Ablenkmagnet wird realisiert, um sicherzustellen, dass der Diffusor im Röntgenmodus garantiert im Strahlengang ist
- Die "*malfunction xx*"-Meldungen werden durch verständliche Meldungen ersetzt
- Als Editiertasten werden nur noch Pfeil-links, Backspace und RETURN zugelassen; alle anderen werden deaktiviert
- Ein Fußschalter wird ergänzt, den der Bediener zum Bewegen des Aufbaus treten muss, um versehentliche Bewegungen zu vermeiden
- 23(!) andere Änderungen an der Software, um ihre Zuverlässigkeit zu verbessern
- Die Handbücher werden angepasst

Basisirrtümer bei Therac-25

Freie Universität Berlin

- Ende der Fallstudie.
- Was haben wir nun gelernt?

- Den Vorkommnissen lagen mehrere grundlegend falsche Verhaltensweisen zu Grunde:
  1. Anfangs zu hohes Vertrauen in die Sicherheit des Systems
  2. Voreiliger Glauben, die tatsächliche Ursache eines Unfalls aufgedeckt zu haben
     - z.B. Versagen eines Mikroschalters beim Unfall 2
  3. Die Annahme, dass das Beseitigen eines bestimmten Fehlers künftige Unfälle verhindern könne

"For every credibility gap, there is a gullibility fill."

(Amerikanische Redensart)

Urgründe der Unfälle

Freie Universität Berlin

- Tatsächlich liegen wirklichen Unfällen fast immer komplex interagierende Ereignisse zu Grunde
  - Mit Urgründen in technischen, menschlichen und organisatorischen Faktoren

- Im Falle Therac-25 z.B.:
  - Fehlende Geschäftsprozesse zur vollen Nachverfolgung gemeldeter Vorfälle
  - Zu hohes Vertrauen in Software;
    Entfernen von Hardware-Sperrmechanismen (interlocks)
  - Schwache Software-Entwicklungspraktiken
    - Hier in Form von Kodierfehlern
    - Oft ist aber wichtiger:
      falsch oder unvollständig erhobene Anforderungen
  - Unrealistische Risikoanalysen und zu hohes Vertrauen in deren Ergebnisse

Probleme bei Therac-20, Folgerungen

Freie Universität Berlin

- Eine andere Untersuchung fand später ganz ähnliche Softwarefehler in der Software von Therac-20
  - die ja mit der von Therac-25 verwandt war
- Folgen des Auftretens war aber maximal ein Herausfliegen der Sicherung
  - aber keine Unfälle
  - denn Therac-20 hatte Sicherheitsschaltungen in Hardware, die unabhängig von der Software eingriffen
- Was lernt man daraus?
  - **Konzentration auf einzelne Softwarefehler führt nicht zu einem sicheren System**
  - Die Gesamtkonstruktion muss sicher sein

Ratschläge an Ingenieure

Freie Universität Berlin

1. Die Systemarchitektur muss Sicherheit auch bei Softwarefehlern sicherstellen können

2. Vertraue Software so wenig wie möglich
   - Benutze Redundanz und Hardwaremechanismen

3. Halte Deine Entwürfe so einfach wie möglich
   - Komplexität erzeugt unerwartete Wirkungen

4. Dokumentation, Dokumentation, Dokumentation
   - Und zwar von Anfang an

5. Baue in kritische Systeme Protokollmechanismen ein
   - Sonst kann man aus Problemen zu wenig lernen

Ratschläge an Ingenieure (2)

Freie Universität Berlin

6. Teste und analysiere deine Einzelteile
   - Nur Systemtest machen ist nicht ausreichend

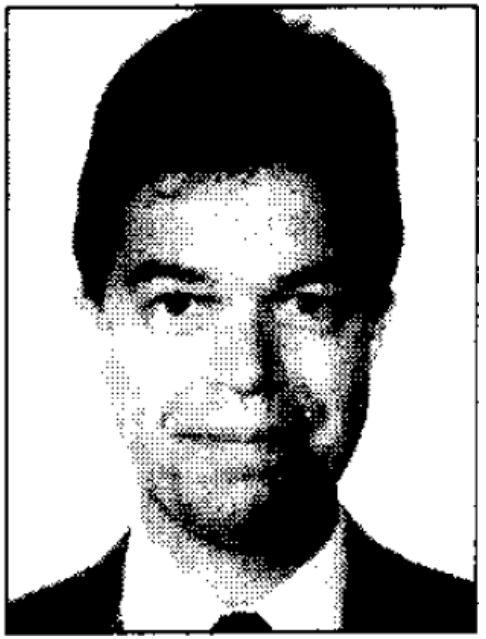
7. Vermeide quantitative Risikoanalysen
   - denn die können sehr irreführend sein

8. Erlerne den Entwurf von Benutzungsschnittstellen
   - denn Fehlbedienung ist oft sicherheitskritisch

9. Opfere nicht Sicherheit für Bequemlichkeit.

Quelle

- Nancy Leveson, Clark Turner:
  "An investigation of the Therac-25 accidents",
  IEEE Computer, pp. 18-41, July 1993.
  - Leider ist der Artikel im Detail oft schwer verständlich
  - Viele der Aussagen in diesem Foliensatz sind durch Deduktion mühsam aus dem Artikel hergeleitet



Inzwischen alles besser geworden?

Freie Universität Berlin

Nein, es gibt deprimierende Wiederholungen:

- 2010: Mehrere Schwerverletzte durch Strahlentherapiegeräte von Varian
  - Ursache: Kollimatortest fehlgeschlagen! ("jaws")
  - Erste Lösung: Ein Warnaufkleber!
  - Grund sind wohl Integrationsprobleme zwischen mehreren beteiligten Rechnern und die Nachrüstung von Hilfsmitteln

Quelle:

http://www.nytimes.com/2010/12/29/health/29radiation.html

http://www.nytimes.com/interactive/2010/12/28/us/radiation-graphic.html

Danke!