Vorlesung "Auswirkungen der Informatik"

Geschäftsprozesse und Sicherheit

Lutz Prechelt
Freie Universität Berlin

- Fallbeispiel "Nachbessern im Betrieb": Therac-25
  - Die Unfälle
  - Maßnahmen-Chaos
  - Zweite Erkenntnis: Gesamtsystem muss sicher sein
- Fallbeispiel "Entwicklungs-management": London Ambulance Service
  - Big-Bang-Fehleinschätzung
  - Mangelnde Einweisung der Benutzer
  - Probleme durch Vertrauensmangel

Definition "Geschäftsprozess"

- Hier:
  In einer Organisation (Firma, Behörde, Verein o.ä.)
  die Vorgaben für die Abläufe, die in der Organisation
  zur Abhandlung einer gewissen wiederkehrenden Situation
  passieren sollen.
  - Typ-Ebene.
    Es gibt auch noch die konkreten Abläufe, die dann tatsächlich
    passieren (Exemplar-Ebene).

Thesen: Geschäftsprozesse

- These "Entwicklungsmanagement":
  Zum sozio-technischen System gehört nicht nur der Systembetrieb, sondern auch die Entwicklung und Fortentwicklung.

- These "Managementfehler":
  Die Reparatur von Sicherheitsproblemen wird ohne geeignete Geschäftsprozesse unzuverlässig.

Verhalten, das institutionalisiert sein sollte

Mensch

Prozess

Aufbau

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

- Heute:
  - 2 längere Fallbeispiele wie erkennbare Sicherheitsprobleme nicht gut behandelt wurden
    1. Therac-25 Strahlentherapiegerät
    2. London Ambulance Service Computer Aided Despatch System
  - Betrachtung des Zusammenwirkens verschiedener Bereiche
    - Technische Eigenarten und Probleme
    - Aktivitäten der Benutzer
    - Aktivitäten der Systemgestalter

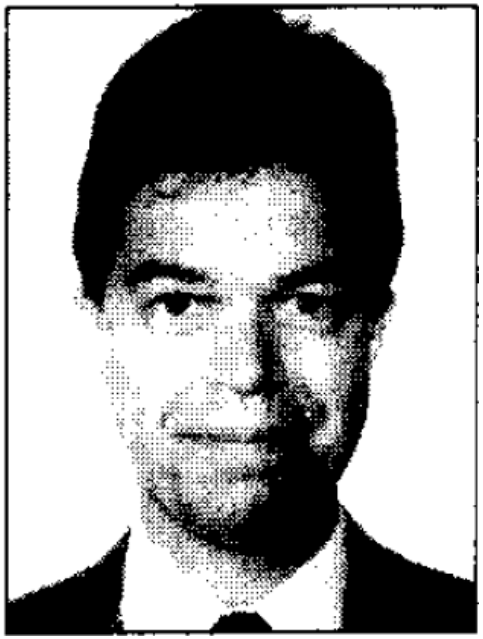
Therac-25

- Strahlentherapiegerät für die Krebsbehandlung
  - Hersteller AECL: Atomic Energy of Canada, Limited
- Ein 25 MeV-Elektronen-Beschleuniger, der Röntgen- oder Elektronstrahlung erzeugt
    - am Markt ab 1982
    - (ein Röntgengerät liefert 0,03 MeV bis 0,15 MeV)
  - Nachfolger von Therac-6 und Therac-20
    - die SW baut auf deren SW auf

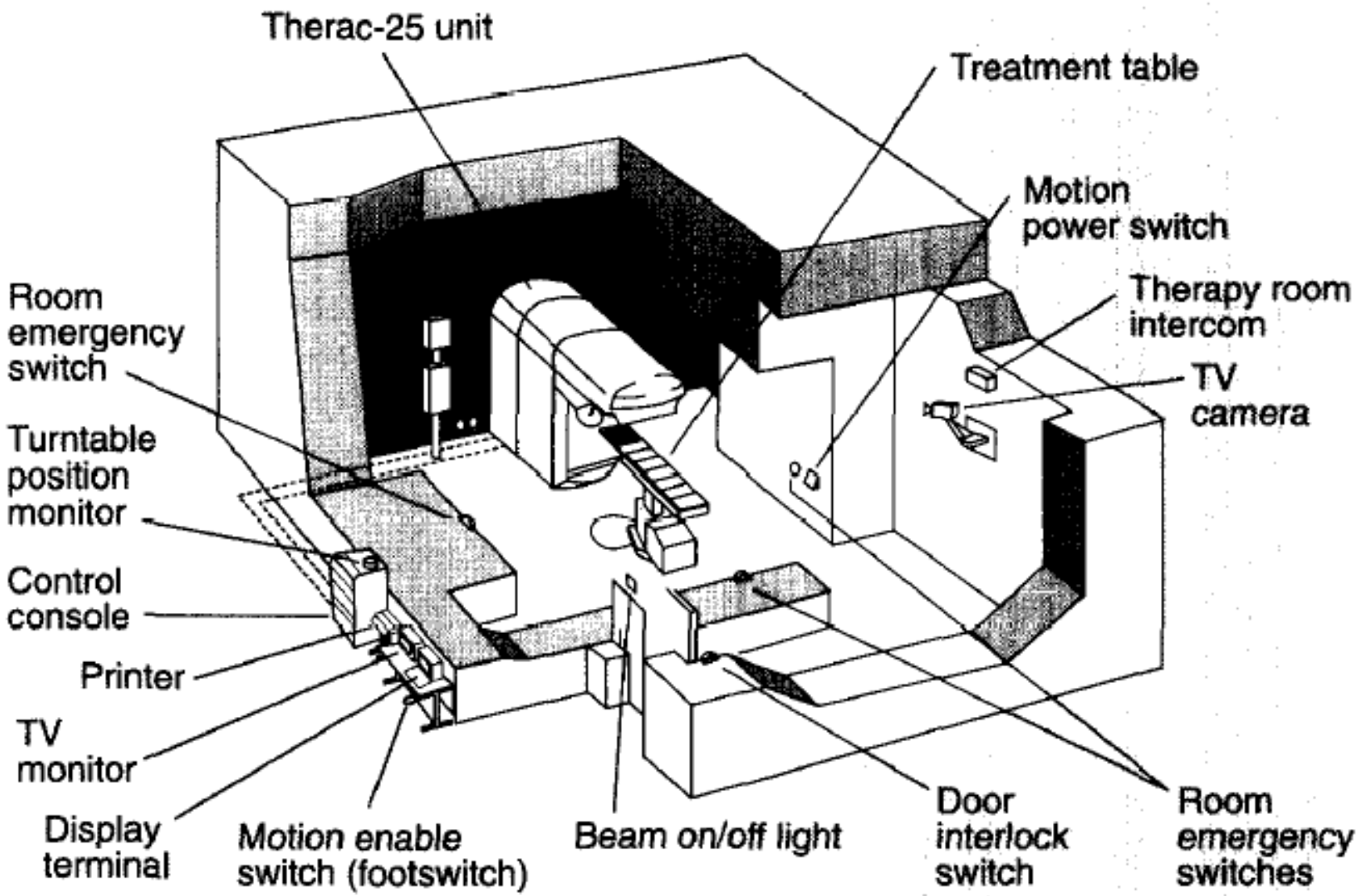
- Erstmals von vornherein mit Computersteuerung entworfen
  - Insbesondere sind nun auch Sicherheitsfunktionen durch Software (statt HW) realisiert:
    - Strahlüberwachung,
    - Dosisbegrenzung

Quelle

- Nancy Leveson, Clark Turner:
  "An investigation of the Therac-25 accidents",
  IEEE Computer, 26(7):18-41, July 1993.
  - Ein Klassiker der Sicherheitsliteratur
  - Leserbriefe und Antworten dazu, sehr interessant!



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 mehrere mit tödlichem Ausgang
- 1987 wurde die Maschine vom Hersteller zurückgezogen und erheblich modifiziert
  - insbesondere wurden wieder Hardware-Sicherheitsmechanismen eingebaut

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

- **Unfallhergang:**
  - 61-jährige Patientin, Nachbehandlung nach Entfernung eines bösartigen Tumors in der Brust
  - Während der Elektronenstrahl-Behandlung
    - Patientin fühlt rotglühende Hitze, sagt "Sie haben mich verbrannt"
    - Techniker: "Das ist unmöglich"
  - Patientin entwickelte starke Rötung und Schwellung
    - In der Behandlungszone und am Rücken an der gleichen Stelle
  - Strahlentherapie zunächst normal fortgesetzt
  - Geschätzte Dosis: 130-200 gray (ein oder zwei Mal)
  - Letztlich:
    - Entfernung der Brust wg. Verbrennung
    - Dauerhafte Lähmung von Schulter und Arm

Exkurs: Strahlungsdosis

- 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
  - Bei Röntgenstrahlung reichen **5 gray** für schwere Gewebeschädigungen

bitte merken

Unfall 1: Marietta 1985 (Fortsetzung)

Freie Universität Berlin

- **Maßnahmen des Krankenhauses:**
  - Krankenhaus-Physiker fragt bei AECL nach, ob Therac-25 theoretisch eine Elektronenbehandlung ohne Strahlauffächerung (scanning) machen könnte ⟹
    - Antwort von AECL nach 3 Tagen: Nein, unmöglich.
  - Sonst aber: Therapie normal fortgesetzt

Prozess

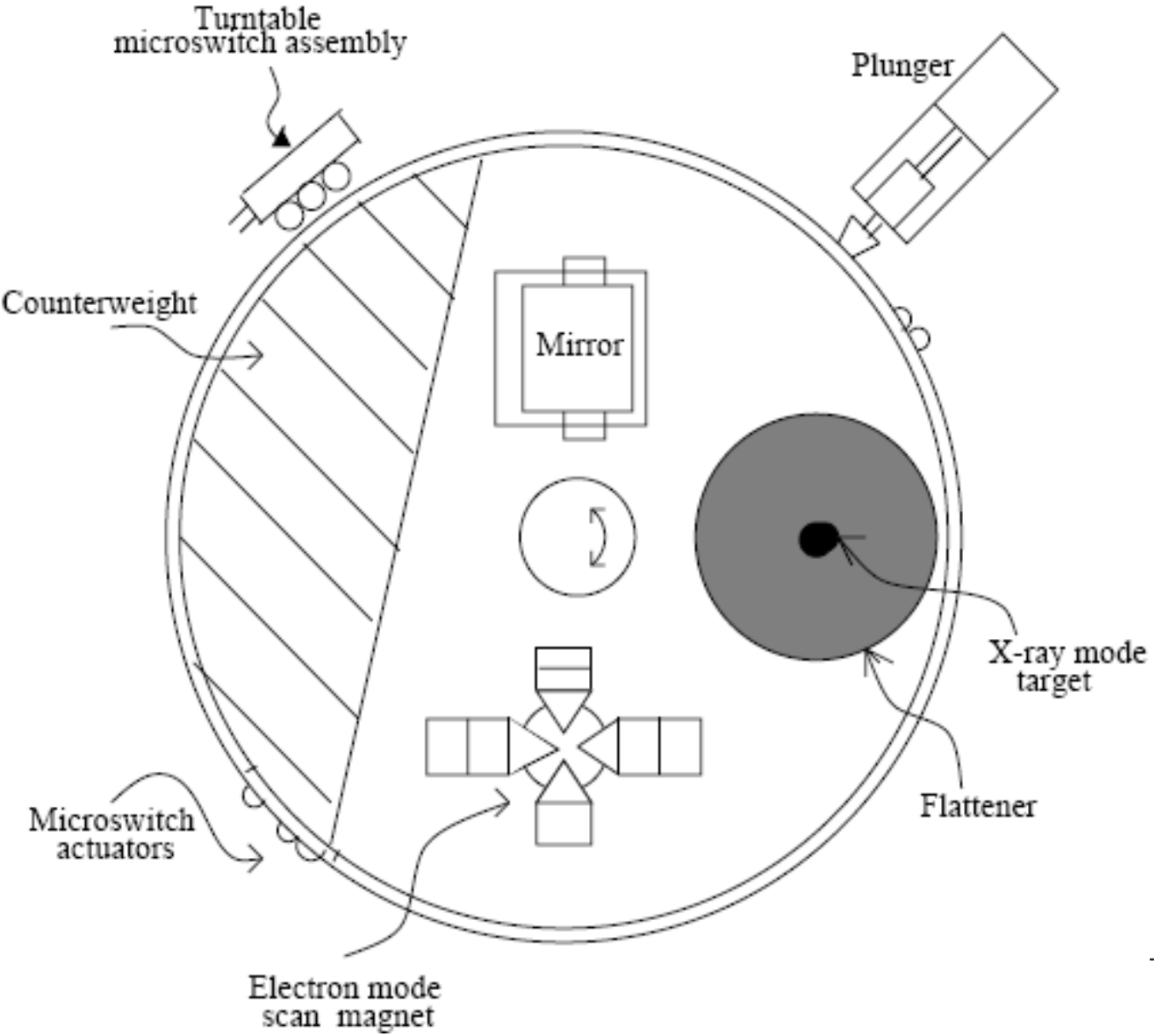
- **Maßnahmen von AECL:**
  - Keine Nachforschungen nach Physiker-Anfrage und von Patientin eingereichter Klage
    - kein Geschäftsprozess ist installiert

Prozess !

  - Meldung an FDA (US-Arzneimittelbehörde) erst nach Unfällen 4 und 5
    - Hersteller (wie AECL) müssen schwere Unfälle melden, Anwender (Krankenhaus) mussten dies nicht bis 1990 nicht

Prozess

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 "Röntgen-Behandlung",
  - in Wirklichkeit jedoch der Drehkranz in Stellung "Patienten-Positionierung" oder "Elektronenstrahl-Behandlung" ist,

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

Exkurs 2: Benutzungsschnittstelle

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,
  - bestätigt dort diese Einstellungen
    - (Gerät hat Sensoren)
  - und gibt die restlichen Daten ein: Patientenkennung, Bestrahlungsbeschreibung (Modus, Energie, Dosis, Dosisrate oder Zeit)

Exkurs 2: Benutzungsschnittstelle (2)

Freie Universität Berlin

```
PATIENT NAME  : TEST                                                    A      1
TREATMENT MODE: FIX          BEAM TYPE: X ENERGY (KeV):                 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: T25VO2-RO3     REASON: OPERATOR        COMMAND:
```

Exkurs 3: Fehlerbehandlung der Therac-25 SW

Freie Universität Berlin

- Stellte die Software einen Fehlerzustand fest, wurde die Behandlung abgebrochen, dabei 2 Arten:
  - "Behandlungspause" (treatment pause):
    - Behandlung kann mit Eingabe "P" (proceed) einfach und schnell fortgesetzt werden
    - Häufig auftretend, normalerweise für Patient ungefährlich
    - Bediener sind Macken der Maschine und das P-Drücken gewohnt
  - "Behandlungsunterbrechung" (treatment suspend):
    - Nach fünf "Behandlungspausen" hintereinander
    - Verlangt ein komplettes Rücksetzen und Neueingabe aller Parameter
- Fehlermeldungen:
  - waren kryptisch: "malfunction 1" bis "malfunction 64"
  - Die Dokumentation enthält anfangs keine Erläuterung dieser Meldungen

Unfall 2: Hamilton 1985

- Ontario Cancer Foundation in Hamilton, Ontario

- **Unfallhergang (1/2):**
  - 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 (Standard)
    - Nach insgesamt 5 Durchläufen direkt hintereinander mit diesem Verhalten: Maschine zeigt "Behandlungsabbruch"
    - Techniker gerufen, fand aber kein Problem an der Maschine
  - Therapie soll fortgesetzt werden

Unfall 2: Hamilton 1985

- **Unfallhergang (2/2):**
  - 25. Termin, 3 Tage später: Patientin klagt über Brennen, Hüftschmerzen und starke Schwellung der Behandlungszone
  - Patientin starb 3 Monate später an extrem virulentem Krebs
    - Obduktion ergab ferner:
      Zerstörung der Hüfte durch die Strahlendosis
  - Geschätzte Dosis: 130-170 gray

- **Maßnahmen des Krankenhauses:**
  - Außerbetriebnahme der Maschine
    - Verdacht auf Strahlenüberdosis
  - Meldung an AECL

Prozess

Unfall 2: Hamilton 1985

- **Maßnahmen von AECL (1/2):**
  - Konnten Versagen nicht reproduzieren
  - 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

Technik ?

Unfall 2: Hamilton 1985

Freie Universität Berlin

- **Maßnahmen von AECL (2/2):**
  - Meldung an FDA und CRPB
    - CRPB: kanadische Strahlenschutzbehörde
    - 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

Prozess

  - Meldung an Therac-25-Anwender:
    "Es gibt ein Problem. Überprüft stets die Drehkranzposition optisch."
  - Die Schranke für "P"-Aktionen wird von 5 mal auf 3 mal gesenkt

Hä?

  - Ein Potentiometer wurde nicht nachgerüstet

Prozess

Unfall 3: Yakima 1985

- Yakima Valley Memorial Hospital in Yakima, Washington
  - 3 Monate nach der Modifikation nach Unfall 2

- **Unfallhergang:**
  - 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
  - Patientin entwickelte Monate später Hautgeschwüre und Nekrose (absterbendes Gewebe) an der Stelle
    - Konnte beides behoben werden
    - Vernarbung, sonst wenig bleibende Schäden

Unfall 3: Yakima 1985

- **Maßnahmen des Krankenhauses:**
  - Suchte intensiv nach der Ursache der Rötung
    - röntgt sogar die Heizdecke der Frau aus deren heimischem Bett, weil deren Heizdrähte als Ursache vermutet waren
  - findet aber keine Begründung

  - Fragte bei AECL nach (telefonisch, brieflich)

- **Maßnahmen von AECL:**
  - Antwort:
    "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."

Prozess

Unfall 4: Tyler 1986

- East Texas Cancer Center in Tyler, Texas

- **Unfallhergang (1/3):**
  - 9. Behandlung eines Patienten mit Rückentumor
  - Sehr erfahrene, schnelle Therac-25-Bedienerin
    - Hat versehentlich "Röntgen" statt "Elektronenstrahl" eingegeben, merkte dies aber vor dem Start und korrigierte die Eingabe mit den Cursortasten
  - Maschine stoppte sofort nach Start mit Meldung "*malfunction 54*" und "Behandlungspause"
    - Das an der Konsole befestigte Merkblatt erklärte diese Meldung mit "*dose input 2 error*", mehr Info gab es auch im Handbuch nicht
      - AECL erklärte viel später, die Meldung könne Überdosis oder Unterdosis anzeigen
    - Konsole zeigte starke Unterdosis an: 6 statt 202 verlangten Einheiten

Unfall 4: Tyler 1986

- **Unfallhergang (2/3)**
  - Der Patient erhielt aber bereits eine Überdosis
    - Er spürte dies (kannte das Prozedere ja) und setzte sich auf
  - An diesem Tag war der Videomonitor zur Kamera des Behandlungsraums nicht angeschlossen und die Sprechanlage defekt
  - Bedienerin ahnte nichts und drückte "P", wie üblich bei Behandlungspausen:
    - Maschine stoppte erneut sofort nach Start erneut mit Meldung "*malfunction 54*" und "Behandlungspause"
  - Patient war noch nicht ganz aufgestanden
    - Daher 2. Überdosis vor Behandlungsabbruch

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

Unfall 4: Tyler 1986

- **Unfallhergang (3/3):**
  - Geschätzte Dosis: 16-25 gray
  - 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: Tyler 1986

Freie Universität Berlin

- **Maßnahmen von AECL:**
  - 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"*

Prozess

Prozess

- **Maßnahmen des Krankenhauses:**
  - Eine unabhängige Firma prüfte die Erklärung
    - Sie befand die Maschine für korrekt geerdet und elektrischen Schocks unverdächtig
  - Der Physiker des Krankenhauses untersuchte Therac-25
    - Fand alle Kalibrierungen und Funktionen intakt
    - Weitere Behandlungen des Tages wurden durchgeführt
  - Maschine ging wieder in Betrieb

Prozess

Prozess

Prozess

Unfall 5: Tyler 1986

- Gleiches Krankenhaus, drei Wochen später

- **Unfallhergang:**
  - Geplante Behandlung: 10 MeV Elektronenstrahl
  - Gleiche 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
  - Patient starb drei Wochen nach dem Unfall;
    Autopsie ergab schwere Strahlungsschäden
    im rechten Hirnlappen und im Hirnstamm

Unfall 5: Tyler 1986

Freie Universität Berlin

- **Maßnahmen des Krankenhauses:**
  - 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

Prozess

- **Maßnahmen von AECL:**
  - konnte das zunächst nicht reproduzieren
    - Erst nach genauer Anleitung gelang es ihnen auch
  - 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

Prozess

Prozess

Die Entwicklung der Therac-25-SW

Freie Universität Berlin

- Aus der Therac-6-SW (Vor-Vorgänger, ab 1972) entwickelt
  - Übernahme durch AECL von Partnerfirma 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

Darüber gibt es inzwischen Vorschriften!

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
  1. Das "Cursor-up"-Problem
     - trat auf wenn nachträglicher Moduswechsel komplett binnen 8 Sekunden nach Ersteingabe abgeschlossen wird
       - also nur bei geübten Bedienern
  2. Das Kollimatortest-Problem
     - trat zeitabhängig auf mit Häufigkeit 1:256

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 Pech
2. Die Ursachen der Unfälle waren schwer aufzuklären,
   - weil die Reproduktion der Umstände schwierig war
   - was daran lag, dass Zeitbedingungen im Spiel waren
3. Ganz zuunterst lagen Programmierfehler
   - aber die sollte man nicht zum Hauptproblem erklären:
4. Das eigentliche Hauptproblem war der Verzicht auf software-unabhängige Sperrschaltungen
5. verstärkt von schlechten Prozessen bei der Aufklärung
   - Keine Prozesse installiert, geringe Handlungsbereitschaft
   - Nachbesserungs-Mentalität

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

- 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 Gegenteil: Die eingegebenen Werte für Strahltyp und Energie nach dem Editieren verändern <u>nicht</u> wirksam die vorherigen Einstellungen. Entweder ist die Korrektur falsch oder das Protokoll ist unzutreffend."*

- Vor Version 3 kam es in Yakima sogar zu noch einem Unfall

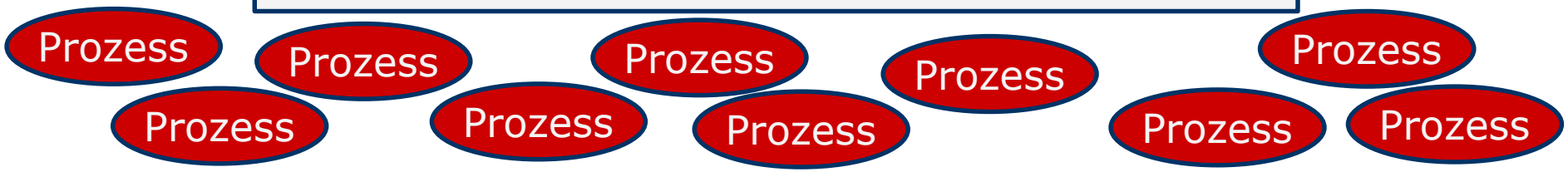
Aktionsplan Version 5, Erkenntnis 1

Freie Universität Berlin

- AECL legte nach insgesamt 14 Monaten die später auch umgesetzte Fassung 5 des Plans vor.

- Inhalt (unter anderem, 34 Punkte insgesamt!):
  1. Kein "p" mehr, immer Neueingabe
  2. Eine Abschaltung nach hohen Einzelpulsen wird in Hardware realisiert
  3. Das Drehkranz-Potentiometer wird ergänzt

Warum braucht es erst Druck einer Behörde, um das zu tun?
Zu schwache Geschäftsprozesse!



Probleme bei Therac-20, Erkenntnis 2

Freie Universität Berlin

- Eine andere Untersuchung fand später ganz ähnliche Softwarefehler in der Software von Vorgängergerät Therac-20
  - die 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 <u>nicht</u> zu einem sicheren System**
  - Die Gesamtkonstruktion muss sicher sein

Ende der Fallstudie.

Ratschläge an Ingenieure

1. Die Systemarchitektur muss Sicherheit auch bei Softwarefehlern sicherstellen können
   - Vertraue Software so wenig wie möglich
   - Benutze Redundanz und Hardwaremechanismen
2. Halte Deine Entwürfe so einfach wie möglich
   - Komplexität erzeugt unerwartete Wirkungen
3. Habe gute Standardprozesse, um mit Mängeln umzugehen
4. Benutze unterstützende Maßnahmen:
   - Dokumentation, Dokumentation, Dokumentation
   - Baue in kritische Systeme Protokollmechanismen ein, sonst kann man aus Problemen zu wenig lernen

Thesen: Geschäftsprozesse

Freie Universität Berlin

2. Beispiel folgt

- These "Entwicklungsmanagement":
  Zum sozio-technischen System gehört nicht nur der Systembetrieb, sondern auch die Entwicklung und Fortentwicklung.

- These "Managementfehler":
  Die Reparatur von Sicherheitsproblemen wird ohne geeignete Geschäftsprozesse unzuverlässig.

Inzwischen alles besser geworden?

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

Zweite Fallstudie:

London Ambulance Service

London Ambulance Service (LAS) Computer Aided Despatch System (CAD)

LAS: ~1400 Notrufe/Tag, ~140 Pers. f. Telefon+Koordination

- (siehe Absatz 2009/2010 der Quelle)

Quelle:

- South West Thames Regional Health Authority: "Report of the Inquiry Into The London Ambulance Service", Februar 1993
  - (nachfolgende vierstellige Zahlen sind Absatznummern darin)

- Bildquellen: LAS, Wikipedia

LAS CAD: Arbeitsweise alt

Freie Universität Berlin

Abfertigung ("despatch") von Notrufen bei LAS bis 1992:

- Despatch Operator (Telefon) erfasst Fakten auf Notizformular
  - ermittelt Ort auf Karte, schickt per Fließband an Zentrale (3002)
- Zentrale: Vereint Duplikate, gibt weiter an Allocator (3003)
  - 1 Allocator pro Bezirk
- Allocator wählt Fahrzeug aus, gibt weiter an Dispatcher (3003)
  - und behält so die Übersicht über Status des Bezirks
- Dispatcher telefoniert mit Station oder gibt weiter an Funker
  - falls Fahrzeug noch unterwegs (3004)

- Verfahren kann flexibel mit Sondersituationen umgehen
- Erlaubte Zeit bis Fahrzeugbenachrichtigung: 3 Minuten (3005)

London Ambulance Service NHS
NHS Trust

LAS CAD: Geplante Arbeitsweise neu

Freie Universität Berlin

- Computer Aided Despatch
  - Unter Nutzung vorhandener Mobile Data Terminals (MDTs) per vorhandenem Radio Interface System (RIFS) (3020)
    - "vorhanden" heißt beschafft in abgebrochenem Projekt aus dem Vorjahr mit Budget £7.5M (3010)
- Automated Vehicle Location System (AVLS)
  - ➔ Despatch nur noch in Ausnahmefällen manuell (3012, 3092)
- Computer Map Display zur Ortsermittlung
  - Was es noch nicht gab: Mobiltelefonie, http, HTML, Google, u.a.

- Konzept benötigt sehr hohe Verlässlichkeit der Technik und des Personals.

Thesen: Geschäftsprozesse (2)

- These "Kein Big Bang":
  Ein komplexes neues System sollte man möglichst nur schrittweise in Betrieb nehmen.

- These "Training":
  Menschliche Bediener brauchen ausreichendes Training für neue Abläufe.

- These "Vertrauen":
  Erfolgreicher Systembetrieb verlangt Vertrauen der Beteiligten in die Tauglichkeit des sozio-technischen Systems.

LAS CAD: Ausschreibung Systementwicklung

Freie Universität Berlin

- Beraterstudie 1990 empfahl f. Lösung m. Standard-SW (3036):
  - Budget £1.5M, Zeitplan 19 Monate.
  - Mit Individual-SW teurer und länger
- Ausschreibung Februar 1991
  - verlangte Inbetriebnahme Januar 1992 (3034)
  - zunächst 35 Interessenten (3034), dann 17 Angebote erhalten (3037)
  - "The standing financial instructions [...] state that the lowest tender should be accepted unless there are 'good and sufficient reasons to the contrary'. The lowest tender was taken." (3031)
  - Die meisten Anbieter waren skeptisch über den Zeitplan (3034)
    - Aber das Management machte Druck (3035, 3040)

Mensch

- Nur 1 Angebot erfüllte alle Kriterien: angenommen
  - Projektbeginn Juni 1991 (3060,3062)

LAS CAD: Umsetzung

Freie Universität Berlin

d.h. sollte anders institutionalisiert sein

- Projekttreffen Juni 1991
  - "the timescale of six months is somewhat less than the industry average for this sort of project which would be more like eighteen months." (3070)
- Qualitätssicherung unterwegs nur informell (3083, 3086)
  - obwohl Tests z.B. für AVLS kompliziert sind (3087)
  - dadurch kein Überblick über die Probleme (s. nä. Folie)
- Termin Januar 1992 verpasst (3088)
- Teillösung Phase 1 in Betrieb genommen: Ortsbestimmung
  - durch diverse Pannen viel Vertrauen beim LAS-Personal verloren (3088)
  - weitere Teillösungen ausgerollt (3089)
  - viele Probleme identifiziert (3090)
- Noch eine Teillösung Phase 2 (3095)
  - beide nur bezirksweise (3097)

Prozess

Prozess

Prozess

Mensch

LAS CAD: Unterwegs aufgedeckte Risiken

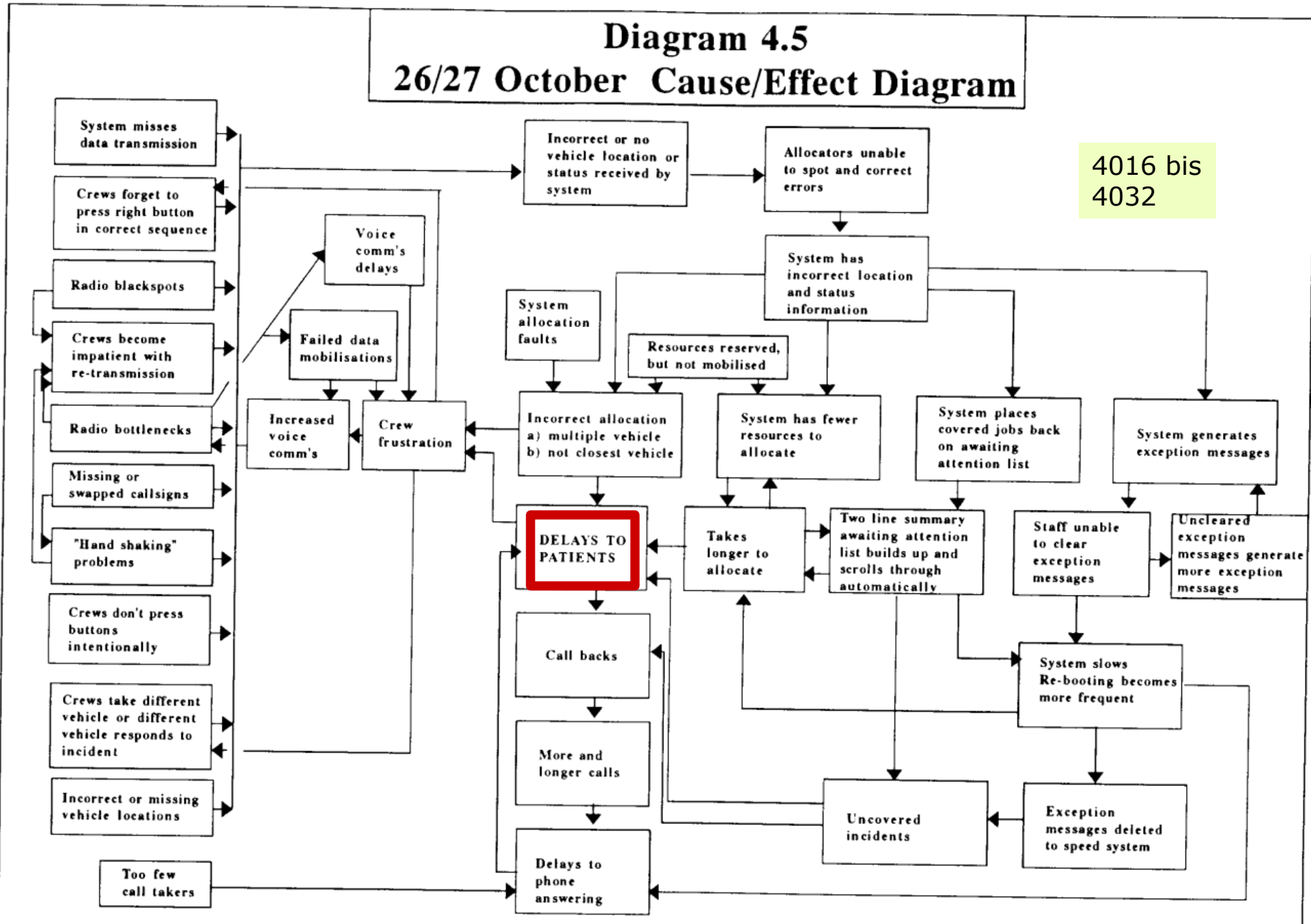
Freie Universität Berlin

3090 (siehe auch 3119-3134):

- Fahrzeugcrews melden Status nicht immer — Mensch
  - Trainingslücken, Technikversagen, evtl. Absicht
- AVLS versagt oft — Technik
  - Gerät falsch installiert, Empfangslücken, Softwarefehler
- System passt manchmal nicht zum etablierten Vorgehen
- Kommunikationsüberlastung beim Schichtwechsel — Umwelt
- Manchmal Einfrieren und Langsamkeit der PCs — Technik
- SW allokiert manchmal nicht das beste Fahrzeug — Technik
- MDTs: Übertragungsprobleme, manchmal Einfrieren — Technik

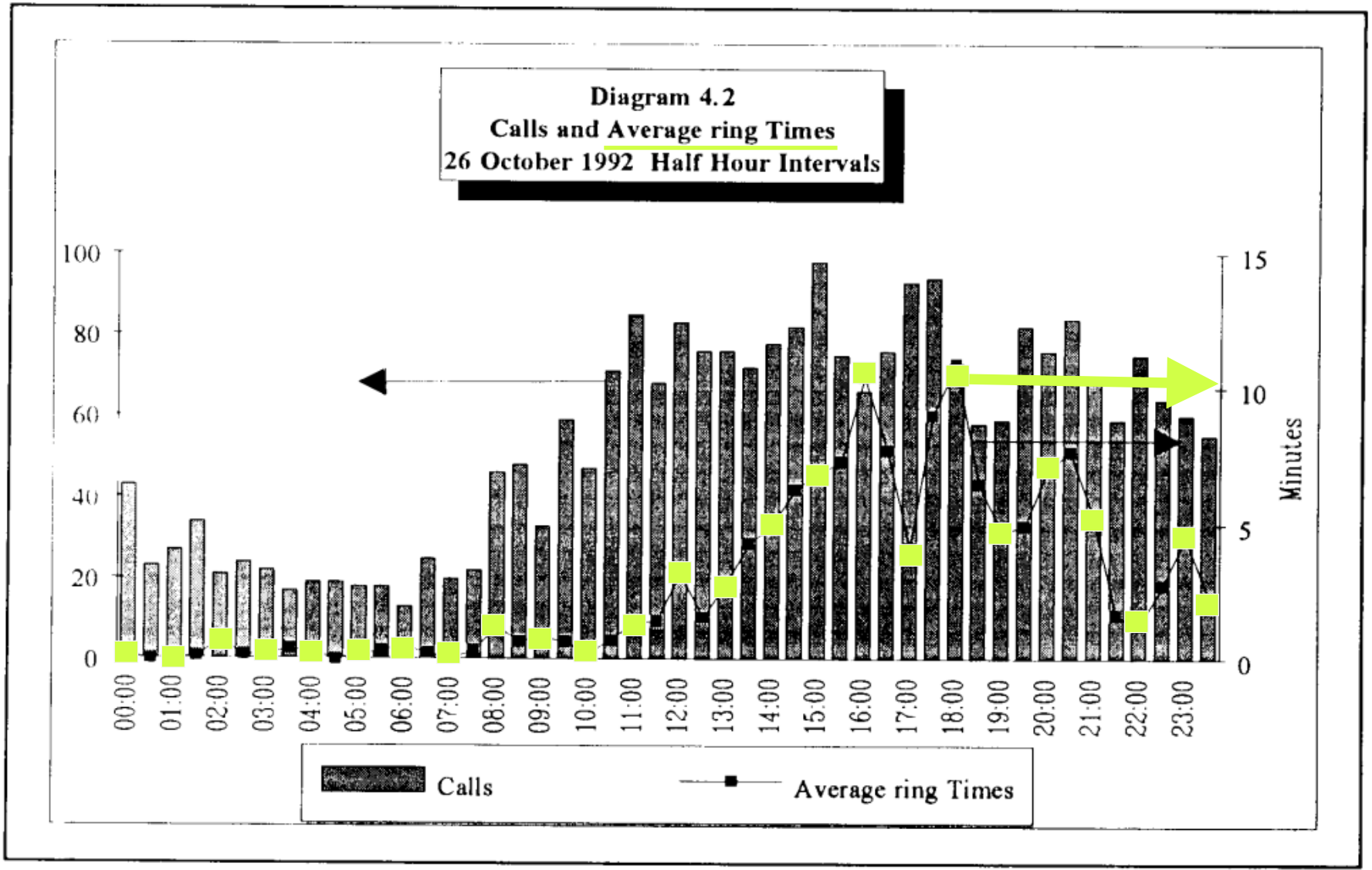
- System lief nie stabil (3098, 3100) — Toleranz, Prozess, Mensch
- Trotzdem fiel die Entscheidung:
  Vollbetrieb Phase 3 in ganz London zugleich starten (3097,3099)

LAS CAD: Ereigniskette bei Inbetriebnahme



LAS CAD: Folgen

- Kein Softwareversagen im technischen Sinne!



LAS CAD: Nachher aufgedeckte Risiken

Freie Universität Berlin

(Siehe auch 4001)

- Fahrzeugbesatzungen wenig eingebunden (3109-3111, 3117) — Prozess
- Zu wenig Training mit dem neuen System (3112) — Prozess
  - und zu sehr separat für die Beteiligtengruppen (3113)
- Kultur von Versagensangst (3115) — Mensch
  - Daher kam auch der Zeitdruck
- Mangel an Vertrauen in das neue System (3118) — Mensch
  - Aus den Mängeln während der Erprobungsphase

Thesen: Geschäftsprozesse (2)

- These "Kein Big Bang":
  Ein komplexes neues System sollte man möglichst nur schrittweise in Betrieb nehmen.

- These "Training":
  Menschliche Bediener brauchen ausreichendes Training für neue Abläufe.

- These "Vertrauen":
  Erfolgreicher Systembetrieb verlangt meist das Vertrauen der Beteiligten in die Tauglichkeit des sozio-technischen Systems.

Erinnerung: Hierarchische Sicht von Unfällen

Freie Universität Berlin

Zum Verstehen eines Unfalls sollte man drei Ebenen unterscheiden:

1. Mechanismen:
   - konkreter Hergang beim Unfall. (Rein beschreibend.)
2. Bedingungen:
   - Zustand des Systems und seiner Umgebung bei Beginn des Unfalls. (Zum Verstehen des Hergangs.)
3. Urgründe (*root causes*):
   - Allgemeine Bedingungen im Umfeld des Systems, die zu den konkreten Bedingungen bei Unfallbeginn geführt haben. (Zum Vermeiden ähnlicher Unfälle in der Zukunft.)

Urgrund-Analyse wird leider selten gemacht, weil Sie fast immer einige Beteiligte beschämt.

LAS CAD: Fazit

- Die technischen Probleme waren erheblich, aber alle lösbar
- Das System hätte aber vor Inbetriebnahme viel länger ausreifen müssen
  - Fehler bei der Entscheidungsfindung!
- Ein **Urgrund** liegt also in den **Managementprozessen**
  - In diesem Fall wurde das im Bericht klar (und erheblich vielschichtiger als hier in den Folien) benannt und ausführlich diskutiert (6005 bis 6092)

Prozess

Danke!