Seminar
Dr. Beckert

Berühmt berüchtigte Softwarefehler
Therac-25

Martin Pfeifer

Universität Koblenz
martin.pfeifer@uni-koblenz.de

Zusammenfassung Eine wichtige Rolle in der Entwicklung von Software spielen Softwarefehler und deren Vermeidung. In diesem Seminar sollen die berühmtesten Softwarefehler vorgestellt und analysiert werden. Ein berühmter Softwarefehler im Bereich der Medizin war unter anderem die Programmierung des Therac-25. Das Therac-25 war ein computergesteuertes Bestrahlungsgerät zur Behandlung von Tumoren. Es wurde in dem Zeitraum von Juni 1985 bis Januar 1987 eingesetzt. Softwarefehler und ganz besonders das fahrlässige Verhalten bei der Fehlersuche und Fehlerbeseitigung führten zu sechs Todesfällen. Die Unglücke zählen zu den schlimmsten in der 35jährigen Geschichte der Strahlentherapie.

1 Therac-25

Das Therac-25 war das dritte Gerät der Therac-Serie. Das Gerät wurde 1984 zum Einsatz freigegeben. Es wurde von der kanadischen Firma Atomic Energy of Canada Limited (AECL) entwickelt und gebaut. AECL war eine staatliche Organisation, die mittlerweile privatisiert wurde. Es wurden elf Geräte vom Typ Therac-25 in den USA und Kanada betrieben.

1.1 Die Vorgänger

Die beiden Vorgänger des Therac-25, das Therac-6 und das Therac-20 waren beide elektro-mechanische Geräte. Das Therac-6 wurde in den frühen 70ern von AECL und der französischen Firma Thomson CGR entwickelt und war ein sechs Millionen Elektronen Volt (MeV) Beschleuniger. Es konnte nur Röntgenstrahlen produzieren. Es besaß auch schon einen Computer, der allerdings nicht für den Betrieb notwendig war. Die Einstellungen wurden direkt am Gerät manuell vorgenommen. So genannte Hardware Interlocks dienten als Schutzvorrichtung. Der Erfolg des Therac-6 führte zu einer Weiterentwicklung, dem Therac-20. Das Therac-20 war ein 20 MeV Beschleuniger. Es konnte schon Röntgenstrahlen und Elektronenstrahlen erzeugen. Im Therac-20 hatte der Computer schon mehrere Aufgaben übernommen, aber er hatte nicht die direkte Kontrolle über die Sicherheitssysteme. 1981 endete die Zusammenarbeit von Thomson CGR und AECL, und AECL entwickelte das Therac-25. Das Therac-25 ist ein dual-mode Linearbeschleuniger, der Röntgenstrahlen mit 25 MeV oder Elektronenstrahlen mit variabler Stärke erzeugen konnte. Es war kompakter und vielseitiger als seine Vorgänger. Der gravierende Unterschied zwischen dem Therac-25 und dessen Vorgängern bestand in der Benutzerführung. Das Therac-6 und das Therac-20 hatten zwar eine Computerunterstützung, aber sie waren Geräte, die ohne Computer auskamen. Im Gegensatz dazu wurden beim Therac-25 die meisten Einstellungen an einer Konsole außerhalb des Bestrahlungsraumes vorgenommen, und es gab auch keine Hardware-Interlocks mehr.

1.2 Das Gerät

Um tiefer gelegenes Gewebe punktuell bestrahlen zu können, muss die Energie durch eine Bleiplatte gebündelt werden. Dadurch, dass die Strahlen erst einmal

die Platte durchdringen müssen, ist eine viel höhere Energie erforderlich (ca. 100fache Energie). Es ist fatal, wenn ein Patient mit Photonen (Röntgenmodus) bestrahlt wird und sich die Platte nicht zwischen Gerät und Patient befindet.

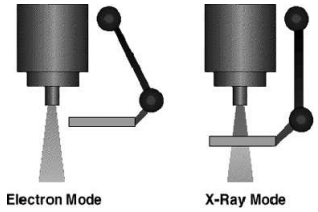

Abbildung 1. Funktionsweise [3]

Ganz grundlegend ist der Satz, dass man den Patienten *soviel Strahlung wie nötig und so wenig wie möglich* zumutet.

Das bedeutet: Um einen Tumor abzutöten, benötigt man eine gewisse Strahlungsintensität. Man darf andererseits die Strahlung nicht zu stark anwenden, um keine benachbarten Gewebe zu beschädigen. Ein Tumor kann aber nur dauerhaft beseitigt werden, wenn alle Krebszellen abgetötet werden.

Für die Behandlung eines Patienten spielte die Drehscheibe eine erhebliche Rolle. Sie konnte drei Stellungen einnehmen, zwei Stellungen waren für die therapeutischen Behandlungen, eine Stellung hatte keine therapeutische Bedeutung, sie diente ausschließlich der Positionierung des Patienten. Ihre Stellung konnte daher auch fatale Folgen für den Patienten haben. Falls sich der Drehteller in der Position für Röntgenstrahlung befand, sich also die Bleischeibe zwischen Gerät und Patient befand, aber eine Elektronenbehandlung durchgeführt wurde, erfolgte eine *Unterdosis*. Dies war der weniger schlimme Fall. Im Gegensatz dazu kam es, wenn sich der Drehteller in der Position für Elektronenstrahlung befand, also die Bleischeibe nicht zwischen dem Patienten und dem Gerät war, zu einer erheblichen *Überdosis* – der schlimmere Fall.

Die Positionierung dieses Drehtellers wurde von einem Computer gesteuert. Der Computer überprüfte die Drehung durch drei Sensoren. Die dadurch gewonnenen Daten wurden anhand der Software kontrolliert. Man hatte auf zusätzliche Hardware Interlocks verzichtet.

Ablauf einer Behandlung. Die Behandlung mit dem Therac-25 begann damit, dass der Patient auf dem Behandlungstisch Platz nahm und vom Techniker in die richtige Position gebracht wurde. Dann stellte der Techniker die notwendigen Parameter ein, hauptsächlich den Behandlungsmodus, die Drehung des Armes und das Bestrahlungsfeld. Bei dem Röntgenmodus konnten die voreingestellten Werte beibehalten werden, während bei dem Elektronenmodus die Intensität manuell eingestellt werden musste. Anschließend wurde der Drehteller in

die entsprechende Position gebracht und die Magneten eingestellt. Dann verließ der Techniker den Raum und gab am Terminal die Patientendaten (einschließlich Behandlungsmodus, Energieniveau, Dosis und Zeit), das Bestrahlungsfeld, die Drehung des Armes und den Behandlungsmodus ein. Um Daten, die sich zwischen Behandlungen nicht verändert hatten, beizubehalten, brauchte der Techniker nur Return auf der Tastatur zu drücken. Die Software überprüfte die Daten und bei Übereinstimmung wechselte der Status von *Unverified* zu *Verified*. Die Behandlung konnte beginnen.

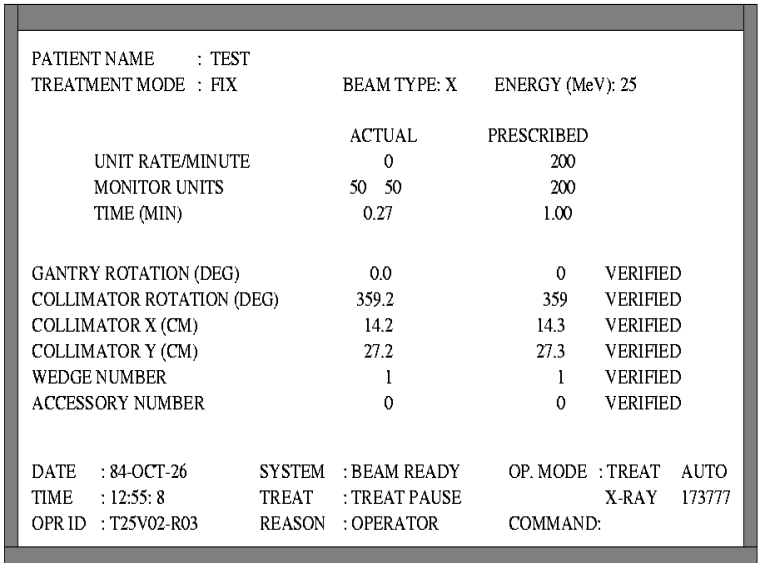

Abbildung 2. Display des Terminals [1]

1.3 Die Software

Die Sicherheitssysteme, die vorher aus elektrischen Stromkreisen und Hardware bestanden, wurden bei dem Therac-25 von einem Computer übernommen. Das Computerprogramm, das aus immerhin über 20.000 Anweisungen bestand, wurde von einem einzigen Programmierer in mehreren Jahren geschrieben. Es wurde nicht bekannt, wer dieser Programmierer war, welche Ausbildung er genossen hatte, oder welche Qualifikationen er besaß. Lediglich sein Ausscheiden aus der AECL 1986 wurde bekannt gegeben. Das Programm war nur unzureichend dokumentiert, und es gab noch nicht einmal Hinweise darauf, dass das Programm getestet wurde, bevor es zum Einsatz kam.

Die Therac-25 Software verwendete kein kommerzielles Betriebssystem. Das eigene Betriebssystem war ein Standalonerealtimebetriebssystem. Es wurde extra für das Therac-25 geschrieben und lief auf einem 32K PDP-11/23.

Die Software, geschrieben in einer PDP-11 Assembler Sprache, hatte vier Hauptbestandteile: die gespeicherten Daten, einen Scheduler, kritische und nicht kritische Aufgaben und eine Interruptroutine. Die Daten bestanden aus der Kalibrierung und den Patienten- bzw. Behandlungsdaten. Der Scheduler kontrollierte die Events und die gleichzeitigen Prozesse, sofern kein Interrupt vorlag. Kritische Aufgaben der Software waren:

- der Behandlungsmonitor (Treat), der das Patienten Setup und die Behandlung kontrolliert und anzeigt. Dazu verwendet er acht Subroutinen in Abhängigkeit vom Wert der Tphase Kontrollvariablen. Die Treats interagieren mit dem Keyboard Handler, der die Kommunikation zwischen Techniker und Konsole regelt (siehe Abbildung 3).
- die Servo Task, der die Bestrahlungsdosis und die Behandlungsparameter verwaltet.
- die Housekeeper Task, der den Systemstatus kontrolliert, verwaltet und auf dem Display anzeigt.

Die unkritischen Aufgaben bestanden unter anderem aus dem Keyboard Prozessor, dem Screen Prozessor und dem Service Keyboard Prozessor (dient der Kommunikation zwischen Behandlungssystem und Techniker).

Die Software hatte den gleichzeitigen Zugriff auf gemeinsame Variablen erlaubt und „Test“ und „set“ waren keine atomaren Anweisungen. Aus dieser Implementation des Multitasking resultierten Race Conditions[1], die bei den Unglücken eine wichtige Rolle spielten.

Das Therac-25 konnte auf zwei verschiedene Arten die Behandlung im Falle eines Fehlers unterbrechen. Auf der einen Seite gab es einen so genannten *treatment suspend*, der das System zurücksetzen und neu starten ließ, und der zweite Weg, die Behandlung zu unterbrechen, war die weniger schlimme *treatment pause*, die aber nur eine einzige Taste (p für proceed) benötigte, um die Behandlung fortzusetzen. Dies konnte man aber nur maximal fünf Mal ausführen, bis das System einen Neustart initiierte.

Die Fehlermeldungen waren kryptisch und bestanden aus dem Wort *Malfunction* gefolgt von einer Zahl von 1 bis 64. Die Fehlermeldungen hatten aber nur in den seltensten Fällen etwas mit der Sicherheit der Patienten zu tun. Laut Berichten eines Technikers kam es bis zu mehr als 40 Fehlermeldungen an einem Tag. Außerdem wurde dem technischen Personal vermittelt, dass es unmöglich sei, einem Patienten eine Überdosis zu verabreichen.

[1] Wenn das Ergebnis mehrerer Ereignisse von deren Reihenfolge abhängt und diese Reihenfolge zeitlich nicht garantiert werden kann, dann spricht man von einer Race Condition. Der Name Race Condition leitet sich davon ab, dass mehrere Prozesse eine Art Rennen um die betroffene Ressource austragen, welches nur einer gewinnen kann.

2 Die Unglücke

2.1 Auswirkungen und Folgen oder die Unglücke

Zwischen 1985 und 1987 kam es insgesamt zu 6 massiven Überdosen, die bei einigen Patienten zum Tode führten. Die ersten Vorfälle wurden seitens der Regierung und des Herstellers nicht untersucht, da eine Fehlfunktion des Gerätes ausgeschlossen wurde. 1987 wurde Therac-25 aber dann letztlich zurückgerufen.

1. Fall: Gorgia, 03. Juni 1985. Eine 61jährige Frau sollte sich in dem Onkologischen Zentrum in Marietta, Gorgia, aufgrund eines bösartigen Brusttumors einer Elektronenstrahlenbehandlung unterziehen. Sie fühlte eine Hitze, als das Gerät anlief. Einige Monate später stellte sich heraus, dass sie eine Überdosis erhalten hatte. Es traten Lähmungserscheinungen im Bereich der Schulter und des Arms auf. Die Brust musste entfernt werden, die Frau verstarb einige Monate später bei einem Autounfall. Der Fehler wurde nie untersucht, AECL schloss Fehler ihrerseits aus. Das Gerät war schon ein halbes Jahr in Betrieb.

2. Fall: Ontario, 26. Juli 1985. Am 26. Juli 1985 sollte eine 40jährige Frau mit Gebärmutterhalskrebs in der Ontario Cancer Foundation Klinik in Hamilton, Ontario, ihre 24. Therac-25 Behandlung erhalten. Der Techniker aktivierte das Therac-25, aber nach fünf Sekunden stoppte das System und gab die Fehlermeldung *H-tilt* aus, das bedeutet, dass es keine Dosis gab und das Gerät sich in der *treatment pause* befand. Der Techniker drückte nach dem Standardverfahren dann die Taste P (für proceed), um das Programm fortzusetzen. Dies geschah allerdings vier Mal, nach dem fünften Mal fuhr sich das System automatisch runter. Sie spürte etwas, einer Verbrennung ähnlich, in ihrer Hüfte. Auf den Verdacht hin, dass es eine Überdosis sein könnte, wurde das Therac-25 runtergefahren. Am 03. November 1985 verstarb die Patientin an den Folgen ihrer Krebserkrankung, aber die Autopsie ergab, dass, wenn sie nicht an der Krebserkrankung gestorben, sie an den Folgen der Überdosis gestorben wäre. Die Überdosis wurde auf 15.000rad geschätzt, statt den gewollten 200rad.

AECL untersuchte die Fehlfunktion, aber sie konnten den Fehler nicht rekonstruieren. Sie vermuteten, dass einer der Schalter defekt war und somit einen Fehler ausgelöst haben könnte. Sie gestanden ein, dass die Mechanik einige Schwächen hätte, und gaben die Weisung, die Stellung des Drehtellers zu überprüfen.

3. Fall: Washington, 11. Dezember 1985. Nach dem Fall in Ontario wurde das Therac-25 in Yakima, Washington von AECL verbessert. Durch einen defekten Microswitch (Schalter, der die Stellung des Drehtellers überprüfte) konnte es zu einem Fehler kommen, d.h. die Stellung des Drehtellers wurde falsch erkannt. Daraufhin wurde eine neue Kontrollsoftware geschrieben, die diesen Fehler bemerken sollte. Die Patientin, die wegen eines Hautkrebses an der Hüfte zur

Behandlung kam, erlitt während einer Behandlung Verbrennungen an der Hüfte. Die Patientin überlebte zwar, muss aber seitdem mit einer steifen Hüfte leben.

Auch dieser Fall hat noch nicht gereicht, um AECL zu alarmieren. Erst die Texas-Fälle einige Monate später warfen für AECL den Verdacht auf, dass es einen Softwarefehler im System geben könnte.

4. Fall: Texas, 21. März 1986. Am 21. März 1986 wurde ein 33jähriger Ölfeldarbeiter mit einem Tumor im oberen Rücken in der Tyler Klinik behandelt. Er sollte mit Elektronen beschossen werden. Der Patient erhielt aber, wie er selber aussagte, einen Schlag, der sich wie ein Elektroschock im Rücken anfühlte. Daraufhin stand er auf, was leider von der Technikerin nicht bemerkt wurde, da das Intercom defekt und die Kamera ausgestöpselt war. Zu dem Zeitpunkt wurde ein weiterer Schuss ausgelöst, der ihn an der Hand traf. Vom System wurde nur der Fehler – malfunction 54 – angezeigt, der Unter- oder Überdosis besagt. Der Patient kam am Abend mit Haut- und Rückenschmerzen wieder in die Klinik. Er verlor die Gewalt über seinen linken Arm, litt an Übelkeit und Erbrechen. Er hatte durch die Überdosis eine Beschädigung des Spinalkanals erlitten, die eine Lähmung beider Beine nach sich zog. Er verstarb im September des gleichen Jahres an den Folgen der Überdosis.

5. Fall: Texas, 11. April 1986. Am 11. April kam ein 66 Jahre alter Busfahrer in die gleiche Klinik, um den Hautkrebs im seinem Gesicht behandeln zu lassen. Er hatte die gleiche Technikerin und die gleiche Maschine wie bei dem ersten Unfall in Texas, aber diesmal funktionierte das Intercom. Als die Technikerin einen lauten Schrei während der Behandlung hörte, eilte sie in den Behandlungsraum. Der Patient sah einen strahlenden Blitz und es roch verbrannt. Sein Gesicht fühlte sich verbrannt an. Drei Wochen später verstarb er. Seine Autopsie ergab eine Überdosis, die den rechten Gehirnlappen und auch das Stammhirn verletzt hatte.

6. Fall: Washington, 17. Januar 1987. Am 17. Januar 1987 erfolgte das letzte Unglück im Yakima Hospital. Ein weiterer Patient erhielt eine Überdosis. Es schien ein völlig anderer Softwarefehler zu sein. Das Ergebnis war aber dasselbe wie vorher. Der Patient sollte eine Elektronenbestrahlung erhalten, erhielt aber eine Röntgenbestrahlung. Im April verstarb der Patient.
(ausführlichere Informationen siehe [1] und [2])

3 Die Fehlfunktion

Für die Überdosis der sechs Fälle waren menschliches Fehlverhalten und zwei völlig verschiedene Softwarefehler verantwortlich.

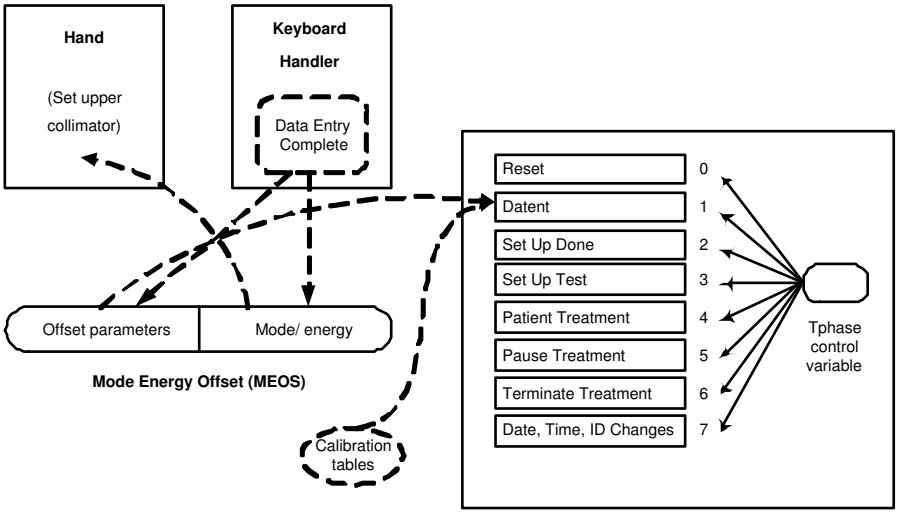

Abbildung 3. Texas Bug [1]

Der Texas-Bug. Ganz besonders der Software Fehler, der für die Texas Unglücke verantwortlich war, zeigt die Schwächen des Designs der Software auf.

Der Behandlungsmonitor (Treat) kontrollierte die verschiedenen Phasen der Programmabarbeitung in den acht Subroutinen. Die Variable Tphase zeigte auf die Subroutine, die abgearbeitet werden sollte.

Eine Subroutine, Datent (data entry), kommunizierte zwischen dem Keyboard Handler und dem System. Dazu griff Datent auf gemeinsame Variablen zu. Der Keyboard Handler erkannte, ob die Dateneingabe vollständig war und setzte dann die „Data Entry Complete“ Flag und Tphase wurde von 1 (Datent) auf 3 (Set Up Test) gesetzt, die dann ausgeführt wurde. Wurde das Flag nicht gesetzt, wurde auch Tphase nicht verändert und das Programm ging wieder in die Hauptroutine.

Die Daten wurden durch einen Cursor eingegeben. Sobald der Cursor alle Eingabemöglichkeiten durchlaufen hatte und am rechten unteren Rand des Displays ankam, wurde das „Data Entry Complete“ automatisch gesetzt. Das Unglück ereignete sich durch einen Eingabefehler der Technikerin, da sie die Möglichkeit hatte, die Daten unverändert zu lassen und durch Bewegen des Cursors zur nächsten Eingabemöglichkeit zu gelangen. Sie hatte nun aus Routine ein x für Röntgenstrahlung eingegeben, obwohl der Patient eine Elektronenstrahlenbehandlung bekommen sollte. Sie bemerkte den Fehler und korrigierte die Eingabe, war aber schon bis an den rechten unteren Rand des Displays gekommen, und ging dann mit dem Cursor zurück, um aus dem x ein e zu machen. Anschließend gab sie die Strahlenintensität ein.

Der Keyboard Handler speicherte die Daten über Modus und Strahlenintensität in einer gemeinsamen Variablen, der zwei Byte großen Mode/ Energy

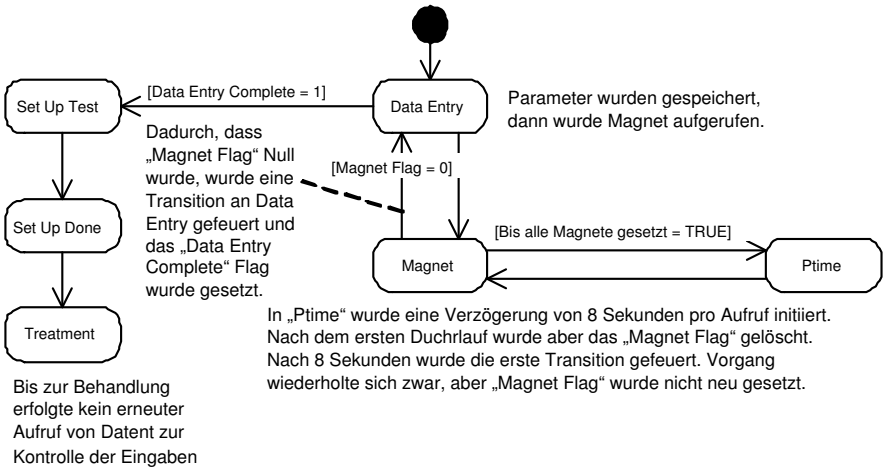

Abbildung 4. Darstellung der Subroutine *Data Entry*

Offset Variablen (MEOS). Das niedrigere Byte wurde auch noch von „Hand“ verwendet, um die richtige Stellung des Drehtellers zu setzen. Wenn aber jetzt die „Data Entry Complete“ durch den Keyboard Handler gesetzt war, wurden Veränderungen nicht mehr erkannt.

Für den Mode/ Energy Offset waren zwei nebenläufige Tasks zuständig, der nicht-kritische Keyboard Handler und der kritische „Task treatment processor“. Das Einstellen der Ablenkmagneten dauerte acht Sekunden. Daher wurde ein Flag gesetzt, dass anzeigte, dass sich die Magnete positionierten und eine Unterfunktion wurde initialisiert, die eine zeitliche Verzögerung bewirkte. Diese Unterfunktion konnte mehrmals aufgerufen werden, bis alle Magnete positioniert waren. Ferner sollte, solange das Flag gesetzt war, überprüft werden, ob die Daten verändert wurden. Diese Flag wurde aber bei dem ersten Durchlauf der zeitverzögernden Unterfunktion gelöscht und somit konnten keine Veränderungen mehr erkannt werden, die nach acht Sekunden, nach Erreichen des Cursors am rechten unteren Rand des Displays, vorgenommen wurden. Die Veränderungen wurden also im System gespeichert, aber sie wurden beim Einstellen des Modus und der Intensität nicht mehr beachtet. Dies führte zu einer ca. 100fachen Überdosis.

Der Texas-Bug wäre sehr einfach zu beheben gewesen. Man hätte das Flag nicht innerhalb der zeitverzögernden Unterfunktion löschen dürfen, somit wären dann zu jedem Zeitpunkt Veränderungen registriert worden.
(siehe [1] und [5])

Der Washington-Bug. Es gab einen zweiten Bug, der für den zweiten Unfall in Washington und wahrscheinlich auch für den Unfall in Ontario verantwortlich war.

Normalerweise lief eine Behandlung so ab, dass der Patient auf dem Behandlungstisch platziert wurde, der Operator verließ daraufhin den Raum und stellte alle Parameter außerhalb des Behandlungsraumes am Terminal ein. Das Therac-25 besaß aber die Möglichkeit, den Patienten anhand eines Positionierungslichtes ganz genau zu platzieren. Zu dieser Feineinstellung befand sich der Operator im Behandlungsraum und stellte die Position direkt am Gerät ein. Dadurch veränderte sich der Status der Parameter von *Unverified* zu *Verified*. Anschließend gab es die Meldung *Press Set Button* und der Bestrahlungsarm brachte sich in die richtige Stellung.

Nachdem die Behandlungsparameter eingegeben wurden und durch die Datent Routine verifiziert wurden, wurde die Set-Up-Test-Routine aufgerufen. Bei jedem Durchlauf der Set-Up-Test-Routine wurde eine gemeinsame Variable *Class 3* inkrementiert. Diese Variable gab an, ob die Stellung des Gerätes verifiziert

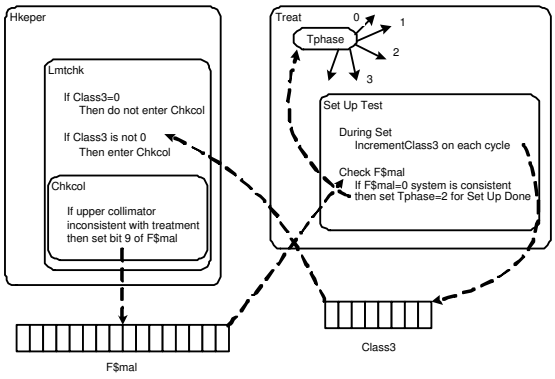

Abbildung 5. Der Washington Bug (aus [1])

wurde. Wenn diese Class 3 ungleich null war, lag eine Inkonsistenz vor und die Behandlung wurde nicht fortgesetzt. War die Variable null, dann bedeutete dies, dass die Parameter mit denen der Behandlung übereinstimmten und die Behandlung konnte begonnen werden. Falls die Class 3 Variable ungleich null war, führte Set-Up-Test weitere Kontrollen des Systems durch Abfragen einer anderen gemeinsamen Variablen durch: F$mal. Wenn diese Variable ungleich null war, gab es eine Fehlfunktion im System, und das Set-Up-Test wurde erneut aufgerufen. Bei null wurde die Subroutine Set-Up-Test beendet und Tphase auf 2 gesetzt (Set-Up-Done-Subroutine) und die Behandlung konnte fortgesetzt werden.

Die Set-Up-Test-Routine konnte aber mehrere hunderte Male aufgerufen werden, bis das Gerät bereit war. Das Problem dabei war, dass bei jedem Aufruf die Variable Class 3 inkrementiert wurde, die aber nur ein Byte groß war. Das bedeutet, dass die Variable maximal den Wert 255 annehmen konnte, was wiederum dazu führte, dass bei jedem 256 Aufruf von Set Up Test Class 3 gleich null

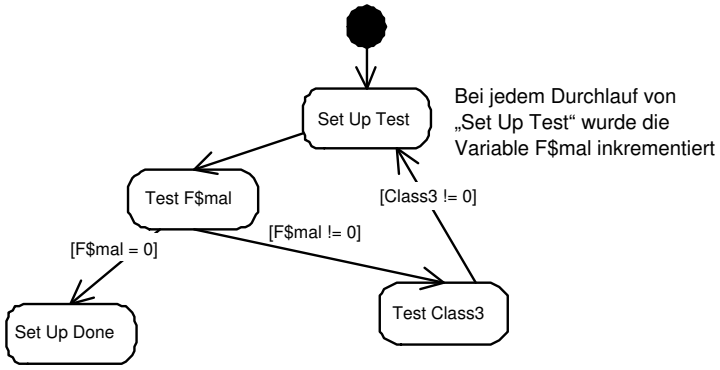

Abbildung 6. Darstellung *Set Up Test*

war, obwohl F$mal noch Fehlfunktionen signalisierte. Dadurch wurde aber nicht mehr überprüft, in welcher Stellung sich der Drehteller bzw. der Strahlungsarm befand, der sich aber noch in der Stellung für das Positionieren des Patienten befand. Die Software initiierte dann die ganzen 25 MeV, obwohl der Drehteller nicht in der richtigen Position war. Ein hoch konzentrierter Elektronenstrahl war die Folge.

Die Lösung dieses Bugs wäre nicht schwieriger gewesen als die Lösung des Texas-Bugs. Man hätte der Variable Class 3 bei jedem Aufruf von Set-Up-Test nur einen festen Wert ungleich null zuweisen müssen ohne Inkrementierung, so dass Inkonsistenz hätte signalisiert werden können, ohne einen Overflow zu bekommen.
(siehe [1])

4 Reaktionen auf die Unglücke

Die Atomic Energie of Canada Limited hat nach dem Bekanntwerden des ersten Unfalles einen Servicetechniker für Untersuchungen in das Krankenhaus nach Gorgia geschickt. Dieser stand in Kommunikation mit der FDA[2] und der AECL. Er konnte den Fehler zwar nicht reproduzieren. Er führte das Versagen auf ein defektes Microswitch zurück, und instruierte alle Benutzer des Therac-25 vor der Behandlung das Gerät visuell zu inspizieren. AECL veränderte die Hardware und behauptete, dass der visuelle Sicherheitscheck nicht mehr notwendig sei.

Nach einem weiteren Unglück in Gorgia im Juni 1985 hatte die AECL gar nicht reagiert, es gab keine Anzeichen dafür, dass AECL die Ursachen des Unglückes verfolgt hat, noch dass es intern irgendeine Untersuchung gab.

Nach dem Unfall in Washington stellte ein AECL-Techniker lediglich fest, dass der Grund der Überdosis nicht am Gerät gelegen haben könnte.

[2] U.S. Food and Drug Adimistration, Department of Health and Human Services

So ging es weiter, bis die Technikerin der Tyler-Klinik in Texas selber Tests am Gerät durchgeführt hatte und die Unfälle und die Sequenzen, die zu ihnen führten, reproduzieren konnte. Die AECL schrieb einen Bericht an die FDA über die Unfälle in Texas. Dann schaltete sich auch die FDA ein, die das Therac-25 als schadhaft erklärte. AECL legte einen Plan zur Behebung des Fehlers vor und erklärte, dass der Fehler behoben sei, und das Therac-25 wurde wieder eingesetzt.

Daraufhin ereignete sich in Washington erneut ein Unfall und AECL sendete einen Techniker, um den Unfall zu untersuchen. Dieser kam zu dem Schluss, dass es einen weiteren Softwarefehler geben musste. Die Geräte wurden im Februar 1987 abgeschaltet. Nach sechs Monaten legte AECL einen neuen Plan zur Verbesserung der Geräte vor, der unabhängige Hardware Interlocks, Softwareverbesserungen und weitere Sicherheitssysteme beinhaltete.

Dieses Verhalten der AECL legt die Vermutung nahe, dass zumindest einige Unfälle hätten vermieden werden können. Es hätten sofort Untersuchungen schon nach dem ersten Unfall vorgenommen werden müssen. Auch hätte man das Gerät schon vor dem ersten Einsatz besser testen müssen. AECL verwendete für die Tests eine „Fault Tree Analysis“ . Dazu mussten die Wahrscheinlichkeiten für die jeweiligen Unglücke berechnet werden und welche Ursachen ein Unglück haben kann. Es liegt auf der Hand, dass es sehr schwierig, umfangreich und damit auch teuer ist, alle möglichen Unfälle und Ursachen zu erfassen. AECL hätte sich auch nicht ausschließlich auf Software bei den Sicherheitssystemen verlassen dürfen. Es hätten ergänzend mechanische Kontrollmechanismen eingebaut werden müssen. Außerdem war der Umgang mit Fehlermeldungen unverantwortlich. Laut eines Technikers gab es pro Tag an die 40 Fehlermeldungen. Diese waren kryptisch und nicht verständlich. Die Anzahl führte auch dazu, dass die Fehlermeldungen nicht mehr ernst genommen wurden. Außerdem war das Vertrauen in die Technik insbesondere in die Software viel zu groß.
(vergleiche [4] und [5])

5 Fazit

Man sollte aus diesen Bugs eins lernen: Man kann ein System nicht sicher machen, wenn man sich nur auf einzelne Software-Bugs konzentriert und diese versucht auszubessern. Vielmehr sollte ein Programm schon bei der Entstehung permanent getestet werden. Die vorgenommenen Tests bei dem Therac-25 waren bei weitem nicht ausreichend. Es kann sich jede komplexe Software unter bestimmten Bedingungen anders verhalten, als es geplant war. Der größte Fehler bei dem Therac-25 war die schlechte Entwicklungspraxis und das Verlassen auf Software in Bezug auf Sicherheitssysteme. Der explizite Fehler im Code ist nicht so wichtig, wie die Unsicherheit im Design von Software im Allgemeinen.

Im Einzelnen heißt das, dass man aus diesen tragischen Ereignissen lernen sollte, und sich Gedanken über die Fehlermeldungen machen muss. Es kann nicht ausreichen, Fehlermeldungen nur zu implementieren, die aber nicht aussagekräftig sind. Wenn sie schon nicht selbstsprechend sind, dann sollten sie wenigstens dokumentiert sein. Dies war aber auch nicht der Fall. Ferner sind teilweise mehr

als 40 Fehlermeldungen pro Tag aufgetreten, was natürlich dazu führte, dass die Fehlermeldungen nicht mehr ernst genommen wurden. Bei der Fehlerbeseitigung sollte man dann auch nicht nur Vermutungen anstellen und anschließend die Symptome der Fehler behandeln, sondern eine fundierte Analyse des Systems durchführen, um die Ursachen der Symptome zu finden, um diese dann zu beseitigen.

Außerdem ist es sehr riskant, die in den Vorgängern des Therac-25 noch vorhandenen Hardware Sicherungen komplett durch Software zu ersetzen. Hardware Lösungen sind oft sicherer und stabiler als softwarebasierte Lösungen.

Auch die Unbekümmertheit, mit der die Personen mit der Technik umgingen muss kritisiert werden. Oft muss erst ein Unfall geschehen, um die Personen auf die Gefahren, die in der Technik stecken können, aufmerksam zu machen. Hinzu kommt die unrealistische Risiko-Einschätzung. Das Gerät wurde nur an einem Simulator getestet, und es scheint, als wäre die Software nur minimal getestet worden. Ferner wurde auch Software sehr naiv wieder verwendet. Die wieder verwendete Software ist nicht an sich sicher, wenn man sie in ein neues System einsetzt, vielmehr ist die Sicherheit die Qualität eines Systems, in dem sie eingesetzt wird, es ist nicht die Qualität der Software an sich. (vergleiche [1])

Ein weiterer Konflikt war die Zielsetzung der Software. Es wurde versucht, eine bedienungsfreundliche Nutzung zu realisieren, die aber leider zu Einbußen der Sicherheit führte. Die Bedienung des Therac-25 so einfach wie möglich zu gestalten und dabei auf viele Dateneingaben zu verzichten, in der Annahme, dass die Daten die eingegeben werden müssen, umso gewissenhafter bearbeitet würden, schlug fehl.

6 Weitere Fehler

Weitere Softwarefehler im Bereich Medizin:

In der Medizin traten und treten relativ häufig Fehler auf, die auch im Zusammenhang mit elektronischen Geräten und damit auch im Zusammenhang mit Software stehen. Dies kann zum einen daran liegen, dass immer neuere Technik eingesetzt wird, als auch vielleicht daran, dass das medizinische Personal und die Ärzte im Umgang mit diesen Techniken noch nicht geübt sind bzw. Risiken die in den Geräten und in der damit verbundenen Software nicht richtig einschätzen.

Ein Fehler war:

> „Gleichzeitiges Auftreten eines Software-Fehlers mit einem Hardware-Ausfall bei Dosierung einer Arsen-Spritze Der gesamte Inhalt führte zum Tod des Patienten“[7]

Ferner wurde ein Überwachungssystem für Intensiv-Patienten vom Markt genommen, da die Software Daten den falschen Patienten zugeordnet hatte.
Im North Staffordshire Hospital Centre wurde Anfang 1992 genau das Gegenteil der Unglücke mit dem Therac-25 festgestellt. Ein Programmierer-Fehler war 10 Jahre lang der Grund von 10-30 % zu geringen Strahlendosen bei insgesamt

knapp 1000 Krebspatienten. (vergleiche [9])
Außerdem kommt mittlerweile auch der Einsatz von immer mehr Geräten wie z.B. Mobiltelefonen (die aus diesem Grund auch in Krankenhäusern verboten sind), die durch ihre Signale andere elektronische Geräte stören und so immer mehr Fehlfunktionen sensibler medizinischer Geräte auslösen.[8][10]
Ein weiteres Problem im Bereich der Medizin ist auch das teilweise nicht vorhandene Problembewusstsein beim Datenschutz. So kommt es immer wieder zu Verletzungen des Datenschutzes durch den etwas leichtsinnigen Umgang einiger Ärzte mit elektronischen Medien. (vergleiche [7])
Auf ein weiteren Softwarefehler im Bereich der Medizin wird meine Kommilitonin Tina Walber in ihrem Seminar „London Ambulance Dispatch System und Gepäcktransport am Flughafen Denver“ eingehen, auf das ich hier verweisen möchte.

Literatur

1. Nancy Leveson, University of Washington, *Medical Devices: The Therac-25* aus Leveson, *Safeware: System Safety and Computers*, Addison-Wesley, 1995 `http://sunnyday.mit.edu/papers/therac.pdf`
2. Ivars Peterson, *Fatal Defect*, Vintage Books, 1996
3. Mark Eby, University of Guelph `http://www.uoguelph.ca/~meby/`, 18.06.2003
4. ComputingCases `http://www.computingcases.org/case_materials/therac/case_history` url/Case%20History.html, 18.06.2003
5. Ramon M. Felciano, Stanford University School of Medicine `http://www.smi.stanford.edu/people/felciano/research/humanerror /humanerrortalk.html`, 18.06.2003
6. Ingolf Giese, Gesellschaft für Schwerionenforschung mbH Darmstadt `http://www-aix.gsi.de/~giese/swr/fehler06.html`, 22.06.2003
7. Andreas von Heydwolff, Salzburg (Austria), veröffentlicht am 8. September 1997, `http://ourworld.compuserve.com/homepages/gesundheits datenschutz/dsb.htm`, 22.06.2003
8. H. Bassen et al.: Computerized medical devices. In: *Proc. 7th Annual Conference of IEEE Engineering in Medicine and Biology Society*, Chicago, Sept. 27–30, 1985, pp. 180–185, aus: Prof. Dr. Klaus Pommerening, Johannes-Gutenberg-Universität Mainz, *IT-Sicherheit in der Medizin*, `http://www.uni-mainz.de/~pommeren/Artikel/stmed.pdf`, 22.06.2003
9. Die Netnews-Gruppe „comp.risks“. Archiv auf dem FTP-Server „CRVAX. SRI.COM“ im Verzeichnis „RISKS:“, aus: Prof. Dr. Klaus Pommerening, Johannes-Gutenberg-Universität Mainz, *IT-Sicherheit in der Medizin*, `http://www.uni-mainz.de/~pommeren/Artikel/stmed.pdf`, 22.06.2003
10. Gunhild Lütge: *Amoklauf der Maschinen.* Die Zeit 2. April 1993, S. 23–24, aus: Prof. Dr. Klaus Pommerening, Johannes-Gutenberg-Universität Mainz, *IT-Sicherheit in der Medizin*, `http://www.uni-mainz.de/~pommeren/Artikel/stmed.pdf`, 22.06.2003