Proseminar

Software Desaster
und wie man sie verhindern kann

TUM WS 2002/03

TUM

STS-1 Columbia Launch Delay

Professor: Tobias Nipkow
Betreuer: Gerwin Klein

08.01.2003

Lennart Johansson

Inhaltsverzeichnis

1. Einführung

Am 10.April 1981, circa 20 Minuten vor dem geplanten Start der Columbia STS-1, versuchten die Astronauten und Techniker die Bordcomputer des Shuttles zu starten, aber sie schafften es nicht. Aufgrund eines Softwarefehlers wurde der lange erwartete Start des ersten wiederverwendbaren Raumfahrzeuges verzögert und konnte so erst zwei Tage später, am 12.April 1981 durchgeführt werden. Beginnend mit der Geschichte, wie das erste Space Shuttle entstand, werden in den folgenden Abschnitten sowohl Bau und Missionsziel, als auch der erste Startversuch vorgestellt. Danach werde ich auf die Ursachen der Startverzögerung eingehen und einen Überblick geben, wie die NASA bei der Fehlersuche vorwärts kam.

2. Columbia STS-1

2.1 Das erste wiederverwendbare Raumfahrzeug

„Stellen wir uns ein Auto vor, das sich anständig starten lässt, mit dem wir wunderbar durch die Landschaft fahren können. Prima soweit. Nur Bremsen hat es leider keine. Die einzige Möglichkeit, es wieder anzuhalten: Wir müssen es am Ende der Fahrt gegen einen Baum fahren. Und dann einen neuen Wagen kaufen, wieder ohne Bremsen. Sensationell dämlicher Gedanke? Ziemlich teure Angelegenheit? Wer sich wohl so einen Blödsinn ausdenkt? Naja: Die NASA zum Beispiel.“ So kommentierte Discovery-Channel in einem Bericht die Raumfahrt, die bis zum Anfang der 80er Jahre nach dem Prinzip „Destruction On Arrival“ (Zerstörung bei der Ankunft) funktionierte.
Im Zuge des Kalten Krieges explodierte in den 60er Jahren das der NASA zur Verfügung gestellte Budget und erreichte 1969 seinen Höhepunkt. Nur so konnten die USA den Wettlauf zum Mond für sich entscheiden, nachdem man im Bezug auf die Raumfahrt gegen die Sowjetunion herbe Niederlagen hatte einstecken müssen. So waren die Sowjets zum Beispiel die Ersten, die einen Satelliten, ein Lebewesen, einen Menschen, oder eine Drei- Mann- Besatzung ins Weltall schickten und ebenfalls die Ersten, die den ersten Spaziergang im All machten. Nachdem das öffentliche Interesse nach einigen Mondlandungen allmählich nachließ und das NASA Budget stark gekürzt wurde, erhoffte sich die NASA mit einem neuen Konzept Geld einzusparen: dem Space Shuttle. Am 3. Januar 1972 fiel die Entscheidung zur Entwicklung eines solchen Systems. An diesem Tag verkündete der damalige US-Präsident Richard M. Nixon einen wiederverwendbaren Raumgleiter zu entwickeln. Man erhoffte sich dadurch die Transportkosten für Nutzlasten zu senken, um Anwendungssatelliten, wie Kommunikations-, Wetter- und Erdbeobachtungssatelliten kostengünstiger ins Weltall befördern zu können. Schon seit 1968 arbeitete eine Shuttle-Task-Force an der Verwirklichung des Transport Systems. Von den ursprünglich fünf verschiedenen Ansätzen, fiel die Entscheidung hauptsächlich zwischen drei Kernentwürfen:

- einem wiederverwendbaren Orbiter mit großen Treibstofftanks auf einer konventionellen Raketenstufe, die - leistungsfähiger als die beiden Feststoffraketen - den Orbiter auf eine höhere Geschwindigkeit beschleunigt hätten. Dieses Konzept wurde abgelehnt, da der Orbiter aufgrund der Treibstofftanks zu groß und damit erheblich teurer gewesen wäre.
- bei dem folgenden Entwurf, der zuerst von der NASA favorisiert worden war, diente ein bemanntes Trägerflugzeug dazu, den eigentlichen Raumgleiter an den Rand der Atmosphäre zu bringen, ihn dort auszuklinken und danach zur Erde

zurückzufliegen. Bei diesem vollständig wiederverwendbaren System, wären beide Shuttles wie Flugzeuge auf Flughäfen gelandet.

- einem teilweise wiederverwendbaren System, bei dem zwei Feststoffraketen als Starthilfe dienen (diese können danach wieder aus dem Meer geborgen werden) und ein Treibstofftank vor Erreichen der Erdumlaufbahn abgesprengt wird: dem heutigen Space Shuttle. Der wiederverwendbare Orbiter könnte im Gegensatz zu den herkömmlichen Raketen wie ein Flugzeug auf einem Flughafen landen.

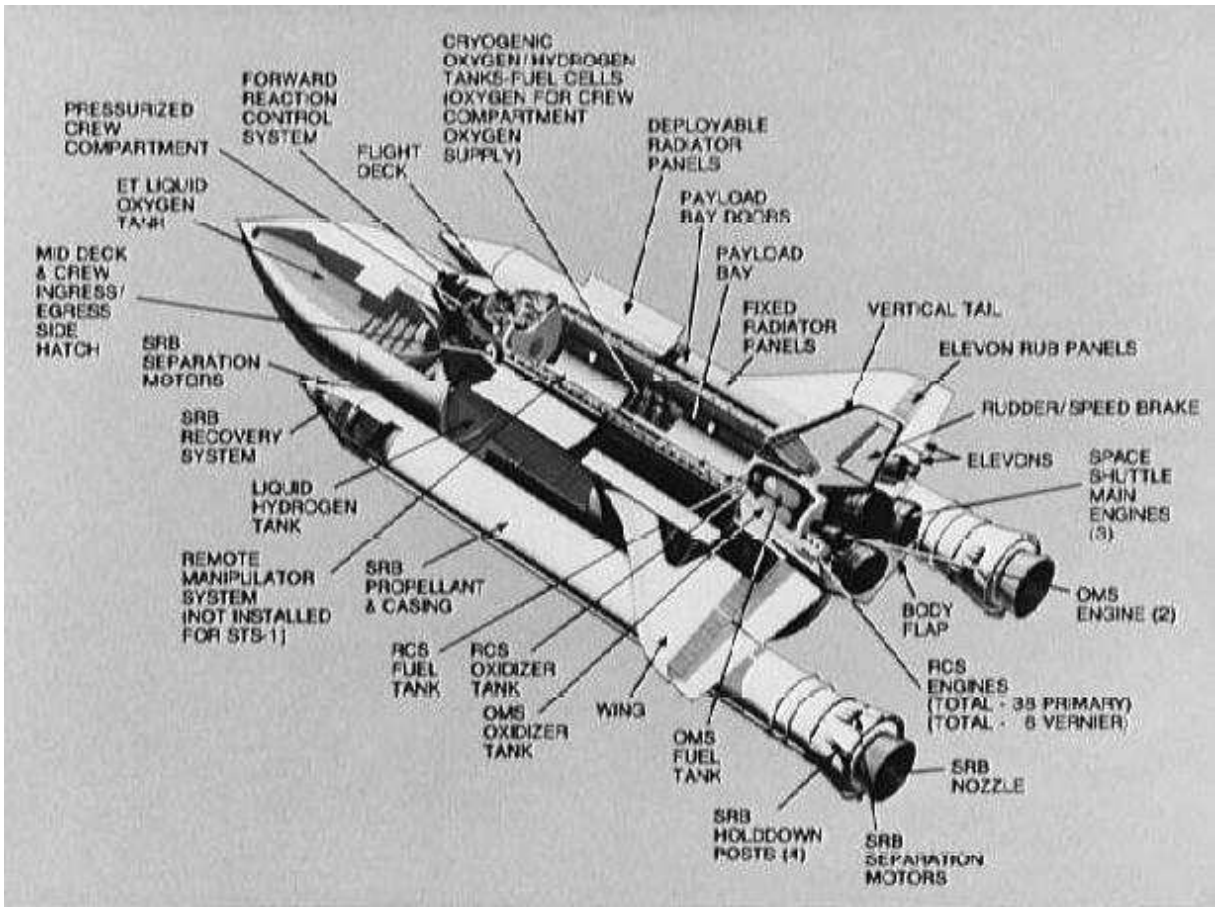
Man entschied sich für die preiswerteste Lösung und erhoffte sich mit dem neuen Space Shuttle die Startkosten im Vergleich zu einer konventionellen Rakete um den Faktor 10 zu senken. Die Entwicklungskosten wurden auf 5,5 Milliarden Dollar geschätzt, die Flugkosten auf 10,5 Millionen Dollar. Die Entwicklungskosten für die Version mit dem Trägerflugzeug hätten bei 14-16 Milliarden Dollar gelegen.
Die ersten Gleitflüge des Orbiters fanden 1977 statt, doch kam es häufiger zu Problemen. Schwierigkeiten machten die Haupttriebwerke des Orbiters, die mit 220 Bar Druck arbeiteten. Das war 3-4-mal mehr, als bei den herkömmlichen Triebwerken. In den Tests fingen sie, ausgelöst durch Probleme in den Turbinen, des öfteren Feuer. Darüber hinaus gab es Probleme mit den Hitzeschutzkacheln, von denen 31000 einzeln angebracht waren. Es wurde klar, das aufgrund der Wartungsarbeiten der ursprüngliche Flugplan von bis zu 60 Flügen pro Jahr nicht eingehalten werden konnte. Schon 1977, vier Jahre vor dem ersten Start, wurde der Startpreis von anfangs kalkulierten 10 Millionen Dollar auf 24 Millionen Dollar revidiert. Die Entwicklungskosten des Space Shuttles hatten sich langsam aber stetig auf 12 Milliarden Dollar in die Höhe geschraubt. Das war mehr als doppelt so viel wie ursprünglich geplant. Der März im Jahre 1978, der anfangs als Starttermin festgesetzt wurde konnte nicht eingehalten werden, so dass der Erststart weiter nach hinten verschoben wurde. Der tatsächliche Startpreis im Jahr 1981 lag dann bei 35 Millionen Dollar. Aber nicht einmal der damalige US Präsident Reagan, der ein erklärter Raumfahrtgegner war und in seiner Amtszeit viele Einsparungen am Budget der NASA vornahm, konnte sich von dem Shuttle als Triumph der amerikanischen Technik lösen. An dem Shuttle-Projekt war neben der NASA außerdem auch das Verteidigungsministerium (DoD) interessiert. Für die Air Force war das Shuttle fest

eingeplant, da ein Shuttle für über 12 t Nutzlast vorgesehen war und so die schweren Kommunikations- und Fotoaufklärungssatelliten des Hexagon transportiert werden konnten. So musste die NASA nicht mehr alle Kosten alleine tragen und dem Jungfernflug der Columbia STS-1 (**S**huttle **T**ransport **S**ystem) stand nichts mehr im Wege.

2.2 Bau und Missionsziele des Shuttles

Das Space Shuttle besteht aus drei Komponenten:

- Der Orbiter: Er ist die einzige Komponente, die voll wiederverwendbar ist. Er hat die Form eines Flugzeuges mit Deltaflügeln, ähnelt also sehr einem normalen Verkehrsflugzeug. Der Raumgleiter ist 37,24 m lang und 17,27m (mit Fahrwerk) hoch. Die Flügelspannweite beträgt 23,79 m. Der Rumpf hat einen Durchmesser von 5,20m. Die Leermasse des Orbiters liegt bei etwa 68 t. Die ursprünglich bei 29,5 t angegebene Nutzlast, die in eine 185 Kilometer hohe Bahn transportiert werden sollte, konnte nicht erreicht werden, da die Leermasse des Orbiters schwerer war, als erwartet. Die Nutzlast betrug dann letztendlich ca. 25 t. In dem Orbiter ist Platz für 2 bis 7 Astronauten. Im vorderen Teil befinden sich das Cockpit und ein 73 Kubikmeter großer Wohnraum. Die drei Haupttriebwerke, durch die der Orbiter angetrieben wird, arbeiten mit Flüssigwasserstoff und Flüssigsauerstoff aus dem Haupttank. Die großen Triebwerke beschleunigen den Orbiter bis zu einer gewissen Geschindigkeit, die nur knapp nicht ausreicht, um ihn in eine Erdumlaufbahn zu bringen. Den Rest übernehmen dann 2 kleine Triebwerke. 5 Computer übernehmen die Steuerung der meisten Funktionen.

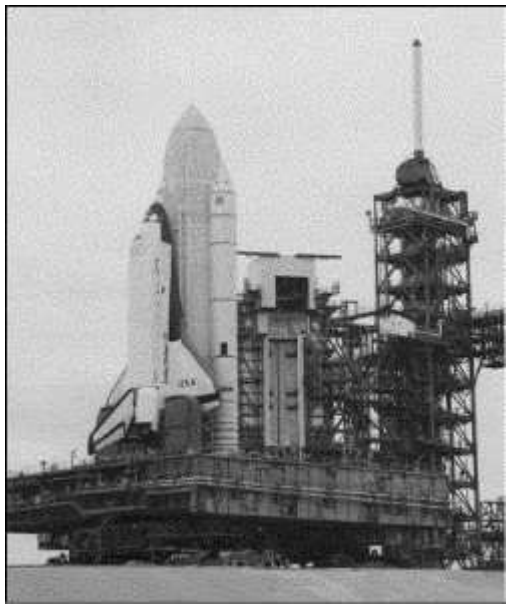


(Skizze des Gesamtsystems)

- Der externe Tank: Er ist die einzige nicht wiederverwendbare Komponente des Space Shuttles. Der 2000 Kubikmeter große Tank enthält über 700 Tonnen Wasserstoff und Sauerstoff für die Haupttriebwerke. Nach einer halben Erdumdrehung wird der externe Tank vom Orbiter abgelöst, damit dieser seine Endgeschwindigkeit erreichen kann. Leer wiegt er nur 35 Tonnen.
- Die Feststofftriebwerke: Beim Start des Gesamtsystems übernehmen zum größten Teil zwei 45,46 m lange und 3,71 m durchmessende, zylindrische Feststofftriebwerke. Jede Feststoffrakete entwickelt einen Startschub von circa 12900 kN. Die Leistung nimmt schon nach 50 Sekunden ab. Nach ungefähr 2 Minuten sind sie ausgebrannt, wobei kleine Triebwerke an der Außenseite dafür sorgen, dass sich die Raketen nach der Abtrennung vom Tank weg bewegen. Sie sind wiederverwendbar, da sie einige 100 km nach einer Fallschirmlandung aus dem Wasser geborgen werden.

Die Aufgaben der ersten Space Shuttle Mission „Columbia STS-1“ lassen sich schnell erklären. Es sollten alle Systeme vom Start bis über die Bedienung und Funktion im Weltraum bis hin zur sicheren Landung auf ihre Einsatzfähigkeit für zukünftige Missionen überprüft und freigegeben werden. Die Plattform DFI (Development Flight Instrumentation), die aus verschiedenen Sensoren und Messgeräten bestand, war die einzige Nutzlast an Bord der Columbia mit dem Ziel, alle Parameter des Orbiters vom Start bis zur Landung aufzuzeichnen.
Während der Missionsdauer von 2 Tagen 6 Stunden 20 Minuten und 56 Sekunden erreichte das Space Shuttle eine Flughöhe von 307,4 km, umkreiste 37 mal die Erde und legte dabei eine Strecke von 1.729.343 km zurück, und das mit einer Geschwindigkeit von 28000 Stundenkilometern.

2.3 Startversuch am 10.04.1981



Der erste Startversuch war für Freitag, den 10. April um 7.00 Uhr morgens vorgesehen. An jenem Tag stand für die NASA viel Geld, aber noch mehr Prestige auf dem Spiel, da es das erste große Projekt seit über einem Jahrzehnt war. Die Columbia türmte sich auf

dem Abschusskomplex 39 des John F. Kennedy Space Center vor Präsident Reagan und der kompletten Fernsehwelt. John W. Young hatte das Kommando an Bord des Space Shuttles. Pilot der Mission war Robert L. Crippen. Doch 20 Minuten vor dem geplanten Start passierte die Katastrophe: der fünfte Computer ließ sich nicht mit den anderen vier Computern synchronisieren. Der Start musste abgebrochen und auf unbestimmte Zeit verschoben werden. Ein Riesenschock für die NASA, der zu einem großen Imageverlust in der Bevölkerung führte. Nun musste die NASA handeln und schnellstmöglich die Ursachen für den verpatzten Start ausfindig machen. Glücklicherweise gelang es noch an demselben Tag die Auswirkungen des Softwarefehlers, der für die Verzögerung verantwortlich war, einzuschränken. So war man sich sicher, dass während eines Fluges der Fehler nicht auftreten könnte. Das reichte der NASA, um den Start auf Sonntag, den 12. April 1981 (also nur zwei Tage später), zu verlegen, auch wenn man die Lösung des Problems noch nicht kannte.

Der zweite Startversuch zur zweitägigen Reise verlief nach Plan. Aber besonders spannend war dann natürlich auch die erste Landung am 14.04.1981. Wenn diese nicht glatt gelaufen wäre, hätte sich der Aufwand nicht gelohnt. Der Pilot hatte nur einen einzigen Versuch, um das Space Shuttle sicher auf die Erde zu bringen. Durchstarten war bei der antriebslosen Landung nicht möglich. Es wurden die zwei kleinen Triebwerke zum Manövrieren verwendet, wobei das Abbremsen auf Landegeschwindigkeit durch Luftreibung geschah. Hier erst kamen die Hitzeschutzkacheln zum Einsatz. Sie erhitzten sich im freien Fall teilweise bis auf mehr als 1000°C. Für das Ausrollen wurden Landebahnen von bis zu 4 km Länge benötigt, da die Landegeschwindigkeit von 340 km/h immer noch deutlich höher lag als bei Verkehrsflugzeugen. Außerdem konnte der Orbiter bei der Rückkehr aufgrund der hohen Belastung nur noch maximal 14,5 t Nutzlast transportieren.

(14. April 1981: Die Columbia kehrt heim)

3. Ursachen der Startverzögerung

3.1 Schwierigkeiten bei der Integration des 5. Computers

Wie schon oben erwähnt, steuerten 5 Computer die wichtigsten Funktionen im Space Shuttle, wobei der fünfte Computer an Bord der Columbia mit einer komplett anderen Software arbeitete, als die anderen vier Computer. 20 Minuten vor dem vorgesehenen Start wollten die Astronauten und Techniker die Software des fünften Computers initialisieren, aber die Initialisierung schlug fehl. Wie sich herausstellte, war es nicht möglich die Software BFS (Backup Flight Control System) im fünften Computer mit dem PASS (Primary Avionics Software System) in den anderen Computern vernünftig miteinander zu verknüpfen. Der Grund dafür war ein kleiner und sehr unwahrscheinlicher Fehler in der Initialisierungslogik des PASS.
Eine Frage zum Beispiel ist, was bei dem Bau des Orbiters unternommen wurde, um einen möglichst hohen Grad an Zuverlässigkeit zu erreichen. Dies gelang den Technikern, indem sie alle wichtigen Komponenten des Shuttles, wie z.B. die Sensoren, Computer, Software, Datenbusse und Energieversorgungen viermal einbauten. So konnte man im Zweifelsfall Probleme einzelner Komponenten durch Überstimmigkeit erkennen und gegebenenfalls richtig darauf reagieren. Das Ziel, dem es zu genügen galt, hieß „Fail Operational – Fail Safe“ („FO/FS“), was soviel bedeutet wie: Eine Komponente durfte ausfallen. Nach dem Versagen einer Komponente durfte weiter abgestimmt werden, solange eine Mehrheit möglich war. Vier Computer arbeiteten mit identischer Software während kritischer Phasen. Diese Methode war aufgrund der Redundanz sicher vor Hardwareversagen. Gegen einen Ausfall aber, der alle vier Computer gleichzeitig betraf, war man nicht gewappnet. Deshalb kam man 1976 auf die Idee, ein absicherndes, als Ersatz fungierendes System in einen fünften Computer an Bord des Space Shuttles zu platzieren. So entging man der Gefahr, dass bei einem gleichzeitigen Ausfall der ersten

vier Computer der Orbiter während einer kritischen Flugphase zu einer manövrierunfähigen Masse werden würde. An das BFS war für die Astronauten die Möglichkeit gekoppelt zu entscheiden, ob sie entweder die ersten vier Computer oder den fünften Computer zur Steuerung der Systeme einsetzen wollten. Für die Entwicklung vom BFS wurde zwar die gleiche Programmiersprache und der gleiche Compiler verwendet („HAL/S“ – von Intermetrics, Inc., of Cambridge, Massachusetts, unter Vertrag mit der NASA), aber es wurde von einer anderen Organisation hergestellt (Rockwell International, Downey, California, im Gegensatz zu IBM, Federal Systems Division, Houston, Texas, für das PASS). Außerdem benutzten sie vollkommen unterschiedliche Betriebssysteme. Die beiden Systeme standen nach folgendem Prinzip miteinander in Verbindung: wenn das BFS nicht die Kontrolle innehatte, hörte es dem Datenverkehr des PASS zu, wusste also ständig über den Zustand des Orbiters Bescheid und war somit jederzeit dazu bereit, die Kontrolle zu übernehmen. Abhängig war es nur von den Informationen, die es von dem PASS erhielt.
Dieses Konzept der Integration brachte einige Veränderungen mit sich:

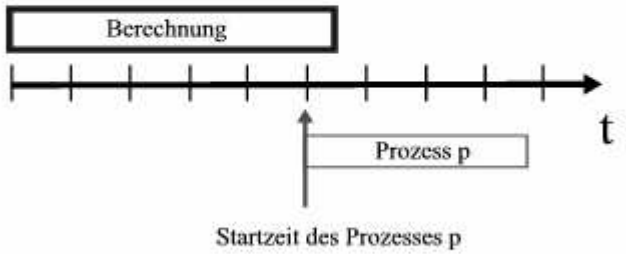
- ein Versagen der ersten vier Computer durfte auf keinen Fall auf das BFS des fünften Computers übergehen, d.h. der fünfte Computer zapfte die Daten der anderen vier nur an, solange es ihn nicht gefährdete.
- nach einem Versagen des PASS konnte nur innerhalb kurzer Zeit die Kontrolle des Raumgleiters an das BFS übergeben werden. Deshalb wurden die Astronauten darauf geschult, ihre Entscheidungen schnellstmöglich zu fällen.
- aufgrund der Integration des BFS mussten einige Abschnitte des PASS angepasst werden. Das PASS Betriebssystem war asynchron und Prioritätsgesteuert. So wurde immer die zu diesem Zeitpunkt wichtigste Aufgabe ausgeführt. Das führte zwar zu vielen Unterbrechungen, aber vier verschiedene Computer waren dennoch dazu in der Lage, identische Dateninhalte aufrechtzuerhalten. Das Ergebnis des aufwendigen Konzepts war ein tolerantes Software System sowohl gegenüber Hardwareversagen (siehe „FO/FS“), als auch gegenüber Softwarefehlern. Im Gegensatz dazu wird jedem Prozess im synchronen BFS ein festes Zeitintervall zugebilligt, in welchem er ausgeführt werden kann. Unglücklicherweise lassen sich synchrone und asynchrone Systeme nicht besonders einfach miteinander kombinieren. Damit das BFS nun alle wichtigen Daten des PASS empfangen konnte, musste das PASS synchron werden oder zumindest synchron erscheinen. Das wurde mit dem kleinstmöglichen Kompromiss im Design erreicht. Innerhalb eines Systemprozesses mit hoher Priorität wurde ein cycle counter installiert. In Anlehnung an diesen wurden alle periodischen Abläufe festgesetzt. Nun schienen für das BFS alle wichtigen Abläufe synchron, nachdem das Zeitintervall der meisten Prozesse konstant und vorhersehbar geworden war.
  Die Veränderungen in dem PASS geschahen in der letzten Entwicklungsphase. Darüber hinaus gab es auch noch einige Prozesse, die nicht dem cycle counter entsprechend verändert worden waren. So war die Unstimmigkeit zwischen dem synchronen und dem asynchronen Software System einer der Gründe für die Startverzögerung.
- die letzte Auswirkung der Integration des fünften Computers war, dass das System noch komplexer wurde. So konnten zwar einige Probleme gelöst werden, dafür sind aber auch andere dazu gekommen. Aber insgesamt war man der Meinung, dass die Verlässlichkeit des Systems gegenüber Softwarefehlern gestiegen war.

3.2 Fehlersuche

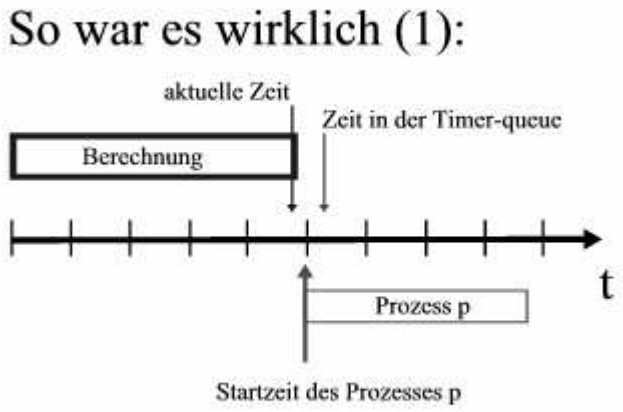
20 Minuten vor dem geplanten Start ließen sich die Softwaresysteme der Computer nicht miteinander synchronisieren. Bis sich IBM eine Stunde nach dem versäumten Start an den Auszügen des PASS zu schaffen machte, dachten zuerst alle, dass sich der Fehler im BFS befindet. Denn das BFS war es ja, das sich weigerte zu synchronisieren, wobei das PASS schon vorher 30 Minuten lang ohne Probleme angelaufen war.
Wenn der erste Computer angeschaltet und das PASS geladen wurde, versuchte er seine auftretenden Abläufe mit der periodischen Ausgabe von den Telemetriedaten des Orbiters zu synchronisieren. Dies wurde erreicht, indem er die Zeit innerhalb des Telemetriesystems las und sich eine Startzeit errechnete, die in der Zukunft lag und die Synchronisation des PASS mit der Telemetrieausgabe zum Ergebnis hatte. Schließlich wurde zum errechneten Zeitpunkt ein Prozess mit hoher Priorität (und zwar der, der den cycle counter enthält) begonnen und alle anderen Abläufe wurden danach bezüglich des cycle counters gestartet. Auch das BFS benutzte diesen und wurde durch den Prozess zeitlich so abgestimmt, dass es wusste, wann es Daten vom PASS zu erwarten hatte, und wann nicht.
Schon freitagmorgens, noch bevor der Start verschoben wurde, stellte man fest, dass einige Prozesse im PASS im Vergleich zu den anderen Prozessen im PASS oder BFS einen Zyklus zu früh stattfanden. Einer war zum Beispiel die Datenabfrage zweier uplink Prozessoren, über die Informationen der Missionskontrolle erhalten werden konnten.
Bald wurde klar, warum das BFS nicht gestartet werden konnte. Für das BFS, das den Datenempfang stoppte wenn es unerwarteten Datenverkehr des PASS vernahm, waren die Daten, die einen Zyklus zu früh kamen, nur unvorhersehbares Rauschen des PASS, auf das Stille folgte, als das BFS seine Daten erwartete.
Am Nachmittag dann, als alle Experten sich ausgetauscht hatten, war der größte Teil des Fehlers aufgedeckt. Immer wenn das Betriebssystem einen Prozess beginnen sollte, dessen Startzeit in der Vergangenheit lag, verschob es den Prozess um so viele Zyklen in die Zukunft, wie benötigt wurden, damit die Startzeit wieder in der Zukunft lag. Die Abfrage der beiden uplink Prozessoren war ein Prozess, der unabhängig von der Startzeitberechnung begann und es konnte nachgewiesen werden, dass in Wirklichkeit die Prozesse des PASS und des BFS der Zeit des Telemetriksystems entsprechend, einen Zyklus zu spät waren. Die Abfrage der Uplink Prozessoren hatte somit zur richtigen Zeit stattgefunden. Jedoch konnte man sich nicht vorstellen, dass die Berechnungen so lange andauerten, so dass der errechnete Zeitpunkt in der Vergangenheit lag, als diese zu Ende waren (s.u. 1.Vermutung). Man wusste aber, dass:

- der Fehler eine sehr kleine Wahrscheinlichkeit hatte und nie vorher im Orbiter oder in Labors aufgetreten ist, auch wenn man in letzterwähnten meistens die teure Initialisierung durch den Gebrauch von „Reset“ umging.
- wenn es gelang, die Computer richtig zu initialisieren, man sich nicht sorgen musste, dass während des Fluges das Problem auftauchen könnte.
- man das System auf den Initialisierungsfehler überprüfen konnte, indem man entweder den Prozess des PASS zusammen mit der Phase der Telemetrieausgabe untersuchte, oder einfach das BFS einschaltete.
- die Synchronisation korrigiert werden konnte, indem man, wenn es nicht funktionierte die Systeme einfach runterfuhr und nochmals einschaltete. Das hätte man am Freitag, am Tag des ersten Startversuchs jedoch nicht machen können, da die Computer mit für das Verhalten des Space Shuttles auf der Startrampe verantwortlich waren.

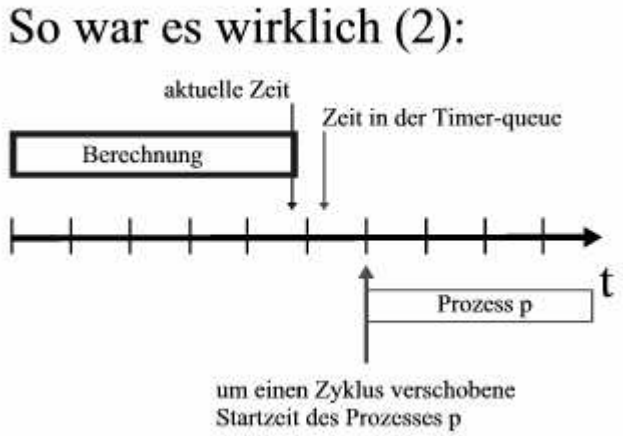
1. Vermutung:



Diese Informationen reichten der NASA aus, um den nächsten Starttermin auf Sonntag, den 12.04.1981 (also nur zwei Tage später) festzulegen.
Erst 8 Stunden nachdem der zweite Startversuch erfolgreich ausgeführt worden war, hatte man die Lösung des Problems gefunden. Die erste Vermutung (s.o.) konnte ausgeschlossen werden. Was war also die Ursache dafür, dass der Zeitpunkt schon vergangen war? Es war die Differenz zwischen der Startzeit und der aktuellen Zeit, die negativ war, so dass die Computer nur annahmen, dass der errechnete Wert schon vorbei war. Damit die PASS Prozessoren in ihrer Zeit übereinstimmten, wurde die sogenannte Timer-queue verwendet, deren erstes Element immer den Zeitpunkt des als nächsten auszuführenden Prozesses enthielt. Da pro Sekunde einige hundert Prozesse stattfanden, zeigte die Timer-queue praktisch immer die aktuelle (ganz wenig in der Zukunft liegende) Zeit an. Der einzige Zeitpunkt, an dem die Timer-queue leer sein musste und mit einem bestimmten Muster initialisiert wurde, war als der erste Computer angeschalten wurde. Aber wie durch eine Laborsimulation gezeigt wurde, war die Timerqueue zu diesem Zeitpunkt nicht leer.
Man hatte vollkommen außer Acht gelassen, dass zwei Jahre vorher eine Veränderung im Gebrauch eines gewöhnlichen Unterprogramms vorgenommen worden war, mit dem Ziel vor der Startzeit Datenbusinitialisierung durchzuführen. Und genau dieses Unterprogramm, das eine Verzögerung hatte, hinterließ eine Zeit in der Timer-queue. Denn die hinterlegte Zeit gab dem Unterprogramm an, zu welcher Zeit es seinen „Schlaf“ beenden und den Betrieb fortsetzten sollte. Dass die Zeit in der Timer-queue danach etwas mehr in der Zukunft lag, hatte damals keine Rolle gespielt. Nun aber, als dieses Unterprogramm an irgendeiner Stelle im System benutzt wurde, konnte durch diese Verzögerung während Kontrollsteuerungen, die bei kritischen Flugsituationen ausgeführt werden, eine zeitweilige CPU Überlastung auftreten. Dieses Problem konnte man ein Jahr vor dem Flug beseitigen. Und zwar wurde die Verzögerungszeit verlängert, damit die Prozesse des Unterprogramms nach der Verzögerung nicht mehr mit den Flugkontrollprozessen zusammenfielen. Durch genau diese Zeitanhebung entstand jedoch die Wahrscheinlichkeit von 1 zu 67, dass die Zeit in der Timer-queue so weit in der Zukunft lag, dass die errechnete Startzeit für die Synchronisation schon vergangen war.



Das Betriebssystem verschob dann einen Zyklus des Systemprozesses nach hinten. Somit waren fast alle (d.h. bis auf die von den Berechnungen unabhängigen Prozesse) darauf folgenden Abläufe in allen Computern um genau diesen einen Zyklus zu spät.



4. Fazit

Stolz waren die Amerikaner auf ihr Space Shuttle. Sie hatten ihrem Auto Bremsen verliehen und erhofften, eine Menge Geld einzusparen. Sie waren sogar so überzeugt und siegessicher, dass zum aller ersten Mal in der Geschichte der Raumfahrt der Jungfernflug eines völlig neuen Systems bemannt durchgeführt wurde. Aber man sieht, dass die NASA damals sehr viel an Prestige zu verlieren hatte, sonst hätte man sich bei der Fehlersuche vielleicht mehr Zeit nehmen können, um den Fehler zu finden, bevor man den zweiten Startversuch unternimmt. Außerdem war es gewiss nicht vorteilhaft, eine so komplexe Software innerhalb einem vorgegebenen Zeitrahmen zu schaffen. Vor allem, wenn man bedenkt, dass die Implementierung der Flugsoftware eine der aufwendigsten war, die bis dahin unternommen wurde.

Quellenverzeichnis

- http://www.bernd-leitenberger.de/poltik-raumfahrt.html
  Version 2.10 vom 09/28/2002 von Bernd Leitenberger

- http://www.bernd-leitenberger.de/space-shuttle.html#ende
  Version 2.10 vom 08/16/2002 von Bernd Leitenberger

- http://www.fbeit.htwk-leipzig.de/kontakte/Fechner/gsn/space8081.html

- http://www.discovery-channel.de/special/mond/zukunft_space_shuttle.cfm

- http://www.guforc.com/news/default.htm?/news/shuttle01.htm

- “The "bug" heard 'round the world”
  Verfasser: John R. Garman
  Herausgeber: ACM Software Engineering Notes
  Erscheinungsdatum: Oktober 1981