Seminararbeit

Seminar: „Berühmt-berüchtigte Softwarefehler“
Sommersemester 2003

Thema: London Ambulance Dispatch System und Gepäcktransport am Flughafen Denver (Logistik)

bei Dr. Bernhard Beckert
Institut für Informatik
Universität Koblenz-Landau

04.08.03

Tina Walber
Mat-Nr. 200210106
Moselweisser Str.10
56073 Koblenz
walber@uni-koblenz.de

Inhaltsverzeichnis

1 Einleitung

Diese Semiararbeit wurde im Rahmen des Seminars „Softwarefehler“ bei Dr. Bernhard Beckert erstellt und beschäftigt sich mit dem Thema „Softwarefehler im logistischen Bereich“. Dabei werden zunächst zwei berühmt gewordene Unglücke, ausgelöst durch Softwarefehler, vorgestellt und anlaysiert: der Softwareausfall beim London Ambulance Service und die verspätete Fertigstellung des Gepäcksystems beim Flughafenbau in Denver. Im Anschluss daran werden Besonderheiten und Schwierigkeiten von logistischen Problemstellungen dargestellt. Der Schwerpunkt liegt dabei auf der Analyse der vorgekommen Fehler und damit der Vermeidung ähnlicher Fehler in der Zukunft.

2 Softwarefehler beim LAS

2.1 Der London Ambulance Service (LAS)

Der London Ambulance Service (LAS) ist zuständig für die Entgegennahme von Notrufen und das Entsenden und Unterhalten von Krankenwagen im Stadtgebiet Londons, er besteht aus einer Zentrale und drei Rettungsstationen die sich in unterschiedlichen Teilen Londons befinden. Gegründet 1930 arbeiteten 1992, im Jahr des Unglücks, ca. 2700 Mitarbeiter beim LAS, am Tag wurden zwischen 2000 und 2500 Notrufe entgegen genommen und bearbeitet, sowie ca. 5000 Patienten täglich behandelt. Der LAS war damit die größte Rettungsdienststelle der Welt. Nach einem Notruf unter der Nummer 999 empfing die CAC (Central Ambulance Control), also die zentrale Kontrollstation, den Anrufer. Hier musste ein Control Assistant (CA) den Anruf auf einem vorgefertigten Formular festhalten. Der Ort des Notrufs wurde anhand einer Stadtkarte festgestellt und im karteninternen Koordinatensystem angegeben. Mit Hilfe eines Fließbandes wurden diese Formulare zu einer zentralen Stelle weitergereicht und dort gesammelt. Sie gelangten so zu einem weiteren Mitarbeiter, der die einzelnen Notrufe - in Abhänigkeit von ihrer Lokalisierung - an einen Zuständigen einer der drei Londoner Rettungsstationen weiterleite. An dieser Stelle wurden auch doppelte Anrufe identifiziert und abgefangen. Für jede der drei Abteilungen war ein weiterer Mitarbeiter damit beschäftigt, mit Hilfe von Informationen über Status und Aufenthaltsort der einzelnen Fahrzeuge zu entscheiden, welches Fahrzeug zu einem Notruf geschickt werden sollte. Zum Sammeln dieser Informationen gab es für jedes Fahrzeug eine „activation box“, in der die Daten über aktuellen Aufenthaltsort und Einsatzbereitschaft, ebenfalls auf Papier, aufbewahrt wurden. Anschließend wurden entweder die Rettungsstationen per Telefon oder direkt die Krankenwagen per Funk verständigt. Der gesamte Prozeß von Anruf bis hin zum Aussenden eines Rettungswagens durfte nicht länger als 3 Minuten dauern.

Dieses Verfahren hatte offensichtlich einige Schwachstellen. Zum einen musste der Aufenthaltsort eines Anrufers von dem CA in einer Karte gesucht werden, was sehr ungenau und zeitaufwendig sein konnte. Auch die Kommunikation, sowohl die schriftliche zwischen den verschiedenen Mitarbeitern mit der Weitergabe von Papier, als auch die mündliche zwischen Zentrale und Einsatzwagen bzw. Station, also mit Hilfe von Telefon oder Funk, war sehr langsam und mühselig. Ein weiterer Schwachpunkt war die große Verantwortung einzelner Personen, bei der Erkennung doppelter Anrufe oder bei der Einschätzung der einzusetzenden Rettungsmaßnahmen.

Deshalb entschied sich das Managment des LAS zur Entwicklung einer neuen Softwarelösung. Dabei sollte dieses System weitaus mehr leisten als andere, bereits existierende und von Feuerwehren oder anderen Notrufzentralen eingesetzte Softwaresysteme. Bereits zu diesem Zeitpunkt stand fest, dass der Erfolg dieser Lösung zu 100% vom Funktionieren und der Zuverlässigkeit der Technik abhängen würde.

Das neue System sollte die folgenden Aufgaben automatisch ausführen:

- Verwaltung der Telefongespräche, Erfassen von Details eines Zwischenfalls, inclusive der Ortsangabe
- Identifizierung der verschiedenen Fahrzeuge, Entscheidung welcher Krankenwagen zu einem Notfall entsendet wird
- Mobilisierung der Krankenwagen und Weitergabe von Informationen an die entsendete Einheit
- Verwaltung der Resourcen, insb. die Lagerung von Materialien und Fahrzeugen (Automatisierung des Verwaltungsprozesses)

Realisiert wurde dieses System mit Hilfe der folgenden Komponenten:

- CAD Hardware, wie die Computer und Bildschirme in der CAC
- CAD Software die auf den Computern der CAC installiert ist
- Lokalisierungssoftware, basierend auf dem Stadtplan von London, zur Bestimmung der Unfallorte
- Funksystem, für die Kommunikation mit den Rettungseinheiten
- Kommunikationsschnittstellen zum Funksystem (RIFS - Radio Interface System)
- MDTs (Mobile Data Terminals) in den Fahrzeugen, die per Spracheingabe bedient wurden und aktuelle Informationen über einen Einsatz anzeigten
- AVLS (Automatic Vehicle Location System) zur Lokalisierung der Fahrzeuge (basierend auf GPS)

Am 7. Februar 1991 wurde das Projekt ausgeschrieben und die Entscheidung fiel auf ein kleines Konsortium bestehend aus den Firmen Apricot, System Options (SO) und Datatrak. Die Fertigstellung sollte am 8. Januar 1992 erfolgen.

2.2 Der Hergang des Unglücks

In den ersten Monaten des Jahres 1992 wurden einige Komponenten der Software in zwei Schritten eingeführt. Am 26. Oktober 1992 um 3 Uhr wurde dann das gesamte System des LAS auf das automatische CAD (Computer Aided Despatch) - System umgestellt. Schon am Morgen zur Rush-hour wurde klar, dass das System nicht den Anforderungen entsprach. So kam es vor, dass Anrufe komplett im System verloren gingen, oder so spät beantwortet wurden, dass Anrufer zum Teil bis zu dreißig Minuten in der Warteschleife des Rettungsdiestes ausharren mussten. Krankenwagen kamen erst nach bis zu drei Stunden am Einsatzort an. Zu anderen Einsätzen wurden zwei Einsatzwagen geschickt.

Am 27. Oktober morgens um zwei Uhr wurde das System zurückgestellt auf ein semiautomatisches System, d.h. Anrufe wurden mit Hilfe des CAD-Systems entgegen genommen, Details über den Notruf wurden allerdings ausgedruckt und wie zuvor weitergereicht, mit der zum Unfallort nächstgelegenen Station wurde das beste Fahrzeug bestimmt, dieses Fahrzeug wurde via CAD benachrichtigt, entweder durch eine Nachricht bei der Basisstation oder durch das Mobile Daten Terminal.

So lief das System weiter bis zum 4. November. Kurz nach 2 Uhr begann das System sich merklich zu verlangsamen um sich kurz danach komplett abzuschalten. Auch nach einem Reboot (es gab keine Möglichkeit zum Backup) war das Problem nicht behoben, das Resultat war, dass Anrufe nicht mehr ausgedruckt werden konnten und die Mobilisierung via CAD nicht mehr möglich war.

2.3 Konsequenzen

2.3.1 Notlösung

Nach dem Totalausfall musste man zu dem manuellen, papier-basierten System zurückkehren. Die Mobilisierung fand, wie zuvor, per Telefon oder Funk statt.

2.3.2 Menschenleben wurden gefährdet

Es ist schwer zu sagen, wieviele Menschen durch die Folgen des Systemausfalls starben. Viele konnten nur zu spät medizinische Hilfe bekommen, Schätzungen zufolge starben bis zu 20 Personen, die durch rechtzeitige Hilfe gerettet hätten werden können.

2.3.3 Imageverlust

Durch massive öffentliche Beschwerden und große Aufmerksamkeit der Medien wurde der Ruf des LAS nachhaltig geschädigt. Z.B. boten, als Reaktion auf das Unglück, private Firmen gegen eine jährliche Gebühr eigene Rettungsdienste an.

2.3.4 Kosten

Die angefallenen Kosten wurden auf 11 Mio Euro geschätzt.

2.3.5 Verantwortliche

Der Geschäftsführer des LAS trat wenige Tage nach dem Unglück nach massiven Beschuldigungen zurück.

2.4 Fehler

Weder das System selbst noch dessen Benutzer waren zum Zeitpunkt der Einführung bereit dazu.

2.4.1 Technische Probleme

- Funktionalität des Systems

  Das System reagierte oft zu langsam und arbeitete dementsprechend nicht immer zuverlässig. Besonders einige bildschirmbasierte Anwendungen reagierten sehr langsam und frustrierten die Benutzer durch sehr lange Antwortzeiten. Diese Probleme waren schon seit der ersten Teileinführung des Systems bekannt, wurden aber nicht behoben.

- Kommunikationsprobleme

  Das System hatte Probleme, sämtliche Daten der Komponenten zu bekommen, z.B. kam es zu inkorrekten oder fehlenden Fahrzeugaufenthaltsorten. Außerdem gab es Probleme mit den „hand shaking“-Routinen zwischen den Mobilen Daten Terminals in den Fahrzeugen und dem Zuweisungssystem, es wurde nicht immer die gleichen Informationen über eine Einheit angezeigt.

- Kontrolle der Anrufe

  Doppelte Anrufe wurden oft nicht erkannt und dementsprechend doppelt behandelt.

- Benutzeroberfläche

  Die Fehlermeldungen häuften sich im Laufe der Zeit, so dass die Listen auf den Bildschirmen der Mitarbeiter immer länger wurden und sogar

aus dem dafür vorgesehenen Bereich herausragten. Außerdem mussten diese Fehlermeldungen auch behandelt (zumindest weggeklickt) werden, was die Telefonagenten zusätzlich beschäftigte. Die Fehlermeldungen wurden dabei nicht nach Prioritäten sortiert, was eine gute Enscheidungshilfe für die Mitarbeiter dargestellt hätte. Ein weiteres Problem war, dass es nicht möglich war bereits bearbeitete Anruf noch einmal zu betrachten, um z.B. festzustellen ob bereits ein Wagen entsendet wurde oder um Angaben zu vervollständigen.

- Funksystem

  Das Funktsystem funktionierte nicht einwandfrei, es gab große Funklöcher. Deshalb wurde es zu einem Engpaß des Systems, die Teams hatten Probleme, sich mit ihren Mobilen Daten Einheiten beim System zu melden.

- Ausdrucke

  Der letzte, totale Systemzusammenbruch kam dadurch zustande, dass die im System verzeichneten Gespräche ausgedruckt und weitergereicht wurden. Ein kleines Programm war für das Ausdrucken zuständig, in diesem Programm befand sich jedoch ein Fehler: Pro Ausdruck wurde eine kleine Datei gespeichert. Innerhalb von zwei Wochen war dadurch sämtlicher Speicherplatz des Systems belegt, und es kam zum Absturz.

- Back-up

  Es gab kein Back-up um im Notfall das Funktionieren des Systems sicherzustellen. Als es zum Crash kam, musste das gesamte System gerebootet werden, was aber nur dazu führte, dass das System nicht mehr funktionsfähig war.

2.4.2 Politische Probleme

- Ausschreibung des Auftrags

  Als im Februar 1991 der Auftrag zur Realisierung des CAD-Systems ausgeschrieben wurde, lag der Schwerpunkt der Auswahlkriterien auf dem Einhalten des Zeitplans und auf dem begrenzten Buget. Da der größte Teil der Anbieter die vorgegebenen Fristen für unrealistisch hielt, blieb letztendlich nur ein Anbieter übrig, das Konsortium bestehend aus Apricot, Systems Options(SO) und Datatrak. Dass es sich hierbei um kleine Firmen handelte, die noch nie ein solches System realisiert hatten, wurde nicht weiter beachtet.

- Technologiesprung

  Das geplante System war sehr innovativ und sollte das modernste der Welt werden. Von verschiedenen Stellen wurde wegen des großen Technologiesprungs von dem Projekt abgeraten, das Managment stand jedoch nach mehreren gescheiterten Versuchen ein Computersystem einzuführen unter Zugzwang und bestand auf dem Projekt.

- Ignorieren von Problemen

  Bereits bei der teilweisen Einführung des Softwaresystems traten Probleme auf. Doch anstatt diese sorgfältig zu untersuchen und vor der Einführung weiterer Komponenten zu testen, wurde die Entwicklung des Projekts vorangetrieben. Auch hier ist wohl der Zusammenhang mit dem unter Leistungsdruck stehenden Management zu sehen.

2.4.3 Probleme in der Planung

- Testläufe

  Das System wurde unzureichend getestet, bevor die gesamte Notrufzentrale umgestellt wurde, das komplette System sogar gar nicht. Die enge Zeitplanung ließ keine Zeit für sorgfältige Tests.

- Mitarbeiter

  Die Mitarbeiter waren nach einigen Problemen mit früheren System und der nicht problemlosen Einführung der ersten Komponenten des Systems bereits frustriert und besaßen kein Vertrauen in das neue System. Sie wurden auch wenig oder gar nicht im Umgang mit der neuen Technik geschult. Der Arbeitsbereich wurde neu strukturiert, die Menschen mussten also in einer neuen Umgebung mit neuen Kollegen zusammen arbeiten, was ebenfalls Unmut unter den Angestellten hervorrief. Zudem gab es zu wenige Mitarbeiter zum Beantworten der Anrufe, so kam es, dass Anrufe verpasst wurden, da die Bearbeitungszeiten länger als zuvor waren.

- Perfekte Informationen

  Das Design des System beruhte auf dem Erhalt perfekter Informationen über sämtliche Aufenthaltsorte der Fahrzeuge und über die Einsatzbereitschaft der verschiedenen Teams. Ohne diese Informationen war eine korrekte Zuteilung der Ressourcen nicht möglich. Die Informationen wurden nicht überprüft bevor eine Entscheidung gefällt wurde. Der größte Teil der Zusweisungsfehler ist auf ungenaue oder inkorrekt Informationen zurück zuführen.

- Schlechte Zusammenarbeit

  Da das Funktionieren des Systems auf immer aktuellen, korrekten Informationen beruhte, war die Zusammenarbeit zwischen den einzelnen Teilen des Systems (Einsatzteams, Zentrale und CAD System) entscheidend. Die Kommunikation unter den verschiedenen Gruppen war allerdings schlecht, der Umgang mit den neuen Geräten und Kommunikationsformen ungewohnt. Ein großes Problem gab es z.B. mit den Einsatzteams, die oft nicht die richtigen Informationen an das System weitergaben. So war es zum Teil schwierig, unter Stress während eines Einsatzes die korrekten Statusinformationen anzugeben. Es kam auch zu Problemen mit der Datenübertragung, so dass die Crews frustriert wurden von immer wiederholten Übertragungen. Desweiteren kam es zu Situationen, in denen ein Fahrzeug genommen wurde, obwohl ein anderes vom System zugwiesen worden war. Die Mitarbeiter sollten über Spracheingabe mit den MDTs kommunizieren. Das war zum einen ungewohnt und funktionierte zum anderen nicht immer, so dass Eingaben oft wiederholt werden mussten.

2.5 Maßnahmen zur Verhinderung

- Beim Entwurf eines solchen Systems sollten die Mitarbeiterbedürfnisse mehr Beachtung finden. Sie sollten beim Design der Benutzeroberflächen einbezogen werden und vor der Einführung entspechend geschult werden.

- Bessere Wartung und genauere Tests der Software während des Betriebs. Der Speicherplatzverbrauch durch die Ausdrucke hätte bemerkt werden müssen.

- Technische Probleme sollten sehr ernst genommen werden, selbst kleine Probleme bei Testläufen können in realen Situation zu großen Problemen führen. Durch ausreichend Test sollten Probleme simuliert und Fehler gefunden werden.

- Entscheidungen sollten auf Kompetenzen beruhen, Experten hinzugezogen und Warnungen ernst genommen werden. Politische Machenschaften dürfen beim Entscheidungsprozess, vor allem in sicherheitsrelevanten Bereichen wie dem Rettungsdienst, keine Rolle spielen.

3 Softwarefehler beim Flughafen Denver

3.1 Der Bau des Denver International Airports

Im September des Jahres 1989 wurde der Bau des Denver International Airport begonnen, der Eröffnungstermin sollte der 18. Oktober 1993 sein.

Er sollte als Ersatz für den Stapleton International Airport dienen. Der Flughafen wurde mit 5 Landebahnen geplant, mit der Ausbaumöglichkeit für 12 Landebahnen. Drei Landungen sollten bei jedem Wetter gleichzeitig möglich sein, 20 Airlines waren an dem Projekt beteiligt. Eine Besonderheit war die große Ausdehnung: die Fläche des Flughafens betrug 53 Quadratmeilen. United Airlines entschied sich sehr früh in der Planungsphase für ein automatisiertes Hochgeschwindigkeitsgepäcksystem. Das alte Gespäcktransportsystem des Stapleton International Airports hatte nur unbefriedigend gearbeitet. Aufgrund der großen Ausdehnung des Flughafens mussten Airlines und Passagieren oft auf das Gepäck warten, Flugzeuge hatten lange Bodenzeiten. Deshalb mussten Airlines Gewinneinbußen in Kauf nehmen, was für den Flughafen einen Imageverlust bedeutete. Für den Gepäcktransport war ein unterirdisches Tunnelsystem vorgesehen. Dabei trat aber zum einen das Problem auf, dass dieselbetriebene Fahrzeuge eines herkömmlichen Systems in diesen Tunneln mit ihren Abgasen die Fahrer und andere Mitarbeiter gefährdet hätte und dass, zum anderen, auf Grund der schmalen Tunnel zwei Wagen nur schwer aneinander vorbeigepasst hätten und vor allem in den Kurven kollidiert wären.

Das neu entwickelte System wurde als „Rettung modernen Flughafendesigns“ begrüßt, man hoffte mit seiner Hilfe größere Flughäfen bauen zu können, da der Transport des Gepäcks bisher das Hauptproblem dargestellt hatte. Obwohl es an anderen Flughäfen vergleichbare Gepäcksysteme gab, war das in Denver einzigartig im Bezug auf Komplexität, Technologie und Kapaziptät.

Das System sollte traditionelle Transportwagen ersetzen und mit mehr als dreifacher Geschwindigkeit auf unterirdischen Schienen selbstständig laufen und damit Geschwindigkeiten über 30km/h erreichen. Die Wagen wurden auch nicht zum Be- und Entladen angehalten, um Energie und Zeit zu sparen. Beim Beladen behielten sie eine Geschwindigkeit von 6,5 km/h bei, beim Entladen sogar von 12,9 km/h.

Die Mitarbeiter klebten beim Einchecken der Passagiere Barcodes in Form von Photozellen auf die Gepäckstücke, auf denen Informationen über den Besitzer, die Flugnummer, das Endziel, über Zwischenstopps und Fluglinie gespeichert waren. Das Gepäckstück wurde dann auf ein Fließband gelegt. Das Fließband hielt das Gepäckstück solange in Bewegung, bis eine Hochgeschwindigkeitsmaschine es genau in dem Moment, in dem ein leerer Wagen ankam, in Richtung des Wagens schoss. Der Wagen fing das Gespäckstück mit seinem Transportkorb auf, der extra zu diesem Zweck in eine Beladeposition gebracht wurde. Diese Methode wurde „Dynamisches Laden“ genannt. Der Barcode des Gepäckstücks im Wagen wurde gescannt und mit Hilfe einer Look-up-Tabelle der Weg zum entsprechenden Gateway bestimmt. Der zentrale Computer leitete dann jeden einzelnen Wagen durch das Umstellen von Weichen zu seinem Ziel.

Eine eigene Software war zuständig für die Koordination leerer Wagen.

Sie wurden bereits an Stellen entsendet, an denen viele Anfragen erwartet wurden, dazu wurde der Strom der Passagiere gemessen. Der zentrale Rechner, der für die Koordination sämtlicher Wagen zuständig war, beobachtete die Position jedes einzelnen Fahrzeugs und empfing Millionen von Nachrichten in der Sekunde. Er schickt auch die Wagen zu speziellen Inspektionsstationen, von denen eine bombensicher ist. Zusätzlich reagiert er auf Behinderungen oder Pannen auf der Strecke und leitet in diesem Fall den Fluss der Wagen um.

Das Transportsystem ist natürlich, die Sicherheit betreffend, ein kritischer Punkt, theoretisch kann der gesamte Flughafenbetrieb durch einen Anschlag auf dieses System gestoppt werden. Um dies zu Verhindern, gab es strenge Zugangskontrollen für Mitarbeiter, die Kommandozentrale war gut bewacht und durch Stahltüren geschützt. Das gesamte System wurde von nur 18 Mitarbeitern betrieben. Zusätzlich wurde ein herkömmliches Gepäcktransportsystem für Notfälle bereitgestellt.

Das gesamte System kostete 193 Mio. Dollar und war mit einer Reihe von Hightech-Komponenten ausgestattet:

- 300 486-Computer in 8 Kontrollräumen
- Datenbank die auf einem fehlertoleranten NF250 Server lief
- Hochgeschwindigkets-Glasfaser-Netzwerk
- 4267 km elektrische Leitungen
- 56 Lasereinheiten (Zum Lesen der Barcodes)
- 400 Frequenzleser (zum Messen des Verkehrs auf den Schienen)
- 35 km Schienennetz
- 10 km Fließband
- 3100 Standardgepäckwagen (450 extragroße)
- 10.000 Motoren
- 92 PLCs (programmierbare Logik-Controller) für die Motoren- und Weichenstellung

Mit dieser Ausstattung war das Denver Gepäcksystem das größte der Welt.

3.2 Der Hergang des Unglücks

Im März 1994 wurde das Gepäcksystem zum ersten Mal in Betrieb genommen, um es der Presse vorzuführen. Das Ergebnis war ernüchternd: Fehler im gesamten System schleuderten Koffer aus den Wagen oder zerstörten

Koffer - „what could go wrong, did go wrong “Die Synchronisierung von Fließband und Gepäckwagen schlug fehl, so dass Koffer nicht aufgefangen wurden. Wagen sprangen aus den Schienen oder stießen zusammen, dabei wurden sowohl die Schienen beschädigt als auch die Inhalte der Koffer herausgeschleudert. Andere Wagen blieben auf der Strecke liegen oder kamen nicht an der vorgesehenen Stelle an, sondern luden ihr Gepäck an einer anderen Station ab. Verlorene Kleidung auf den Schienen verstopfte diese wiederum, wodurch es zu weiteren Behinderungen und Crashs kam. Die meisten Wagen transportierten Koffer mit unlesbaren Barcodes, weshalb sie zur manuellen Sortierung umgeleitet werden mussten. Die Pressenachrichten waren dementsprechen schlecht. Die ausführende Firma BAE analysierte, dass die Probleme des Systems nicht von einem falschen Konzept, sondern von Softwarefehlern und technischen Problemen herrührten. Selbst im August 1994, nachdem schon viele Fehler gefunden und beseitigt worden waren, war die Performance des Systems immer noch nicht ausgereift: Wagen stießen weiterhin zusammen oder sprangen aus den Schienen. Der Fluhafen hätte am 31. Oktober 1993 eröffnet werden sollen, nach mehrmaligem Verschieben dieses Termins wurde der Flughafen am 28. Februar 1995 eröffnet, 16 Monate später als geplant und mit sehr beschränkter Funktionalität.

3.3 Konsequenzen

3.3.1 Notlösung

Das System wurde sehr beschränkt in Betrieb genommen: Ursprünglich sollten alle drei Hallen des Fluhafens von dem neuen System profitieren, ein herkömmliches System wurde nur für den Notfall installiert und sollte den Dienst aufrechterhalten, wenn das erste System nicht funktionierte. Es wurde aber letztendlich nur die Halle A an das neue System angeschlossen, in B und C lief das traditionelles Transportsystem. Hier wurde das Gepäck weiterhin von Menschen sortiert und war dadurch natürlich langsamer. Die Konzeption des automatischen Systems musste so geändert werden, dass Effizienz eingebüßt wurde. Die Kapazität der Strecken wurde von 60 Wagen pro Minute auf 30 herabgesetzt, nur die Hälfte der 84 Gates wurden beliefert, das System erreichte nur 12 Prozent seiner Kapazität. Anstelle von Abfertigen und Weiterleiten von Gepäckstücken konnten nur solche vom System übernommen werden, die in Denver an die Passagiere ausgegeben wurden.

3.3.2 Kosten

Obwohl das System weniger leistete als ursprünglich vorgesehen, kostet das Projekt entschieden mehr als geplant. Vorgesehen waren 193 Millionen Dollar, letzendlich mussten 311 Millionen Dollar für das Gepäcktransportsystem investiert werden. Die Gesamtkosten des Flughafenbaus stiegen von geplanten 1,7 Milliarden Dollar auf 4,5, da der Flughafen so lange nicht eröffnet

werden konnte. Da die Politiker versprochen hatten, die Steuern nicht zur Finanzierung des Flughafens zu erhöhen, mussten sie Anteile des Flughafens verkaufen. Dies wurde allerdings im Laufe der Zeit auch schwieriger, da durch weitere Verzögerungen der Eröffnung und dem Aufdecken von Fehlplanungen der Wert der Papiere sank. Wegen der zusätzlichen Kosten musste eine Fluhafengebühr von 20 Dollar eingeführt werden, damit lag der Denver International Airport landesweit an der Spitze, andere Flughäfen nahmen zwischen 5 und 10 Dollar pro Passagier.

3.3.3 Imageverlust

Das Gepäcksystem, das als innovativ und imagefördernd für den Flughafen begrüßt wurde, stellte sich letztenlich als „a national embarrassment for the city“[7] heraus. Die schlechte Performance des Gepäcksystems, das mehrmalige Verschieben des Eröffnungstermins und der letztendliche Einbau eines herkömmlichen Systems sorgten für viele schlechte Nachrichten in der Presse. Auch die Airlines zeigten sich unzufrieden mit dem Bau des neuen Flughafens.

3.4 Fehler

3.4.1 Politische Probleme

- Politische Entscheidungen

  Die Stadtverwaltung von Denver musste als Generalbauleitung ihre Entscheidungen oft von den Interessen verschiedener lobbyistischer Gruppen abhängig machen, und traf so einige Entscheidungen, die für das Gesamtprojekt eher hinderlich waren. Dass die Entscheidung für das vollautomatische Gepäcksystem fiel, obwohl Experten davon abrieten, ist sicher in diesem Rahmen zu sehen.

- Auftragsvergabe

  Obwohl früh feststand, dass die BAE der geeigneteste Anbieter für den Auftrag war, wurde der Auftrag erst sehr spät (2 Jahre nach Baubeginn) vergeben, es bestanden Zweifel, ob die BAE z.B. genug Frauen und Mitglieder von Randgruppen einstellen würde.

3.4.2 Technische Probleme

- Technologiesprung

  Der technologische Fortschritt vom Vorgängersystem zum vollautomatischen gleicht eher einem Technologiesprung als einer Entwicklung. Die BAE wurde durch die Verwendung moderner Bauteile dazu verleitet, vom System eine perfekte Performanz zu erwarten, sie räumte

keine Spielräume für Fehler ein. Von den einzelnen Komponenten wurde erwartet, dass sie auf höchstmöglichem Niveau arbeiteten. Die enge Kupplung der verschiedenen Komponenten führte zusätzlich dazu, dass es schon beim Versagen einzelner Komponenten zum Stillstand des gesamten Systems kommen konnte.

- Barcodes

  Die Barcodes auf den Gepäckstücken konnten in 70% der Fälle nicht gelesen werden, deshalb musste ein Großteil der Gepäckstücke zu manuellen Sortieranlagen umgeleitet werden. Mit besseren Druckern konnte diese Rate auf 5% reduziert werden. Außerdem mussten die Lesegeräte sehr genau kalibiriert sein, wurden aber durch Handwerker leicht verstellt oder verschmutzt, so dass sie die Barcodes nicht mehr lesen konnten.

- Netzwerkarchitektur

  Die BAE hatte sich für eine heterogene Netzwerkarchitektur entschieden, d.h. MS-DOS bassierte 486er PCs wurden mit Novell Software vernetzt. Der Datenverkehr führte regelmäßig zu Systemabstürzen, deren Ursachen oft im Detail nicht nachvollziehbar waren. Das 10-Megabit Netzwerk genügte nicht um die anfallenden Daten zu transportieren. Letzendlich musste ein 100-Megabit Netzwerk installiert und mit einer geänderten Architektur die maximale Netzlast auf 5% herabgesetzt werden.

- Softwaredesign

  Im Laufe der andauernden Verbesserungen und Modifikationen wurde das Programm zur Steuerung der Anlage sehr komplex. Es wurde für die Programmierer immer schwieriger Fehler zu finden und sinnvoll zu beheben.

- Tunnelsystem

  Die Tunnel waren zu eng, Wagen kollidierten oder blieben stecken. Die Fehlersuche im unterirdischen Tunnelsystem wurde dadurch erschwert, dass die Funkgeräte der Mitarbeiter nicht funktionierten.

- Synchronität

  Die Weitergabe des Gepäcks von Fließband zu Transportwagen funktionierte nicht synchron, Gepäckstücke wurden nicht aufgefangen und fielen auf die Gleise.

- Gepäckwagen

  Aus manchen Wagen fiel das Gepäck heraus. Entweder weil die Klappe zum Halten der Gepäckstücke nicht einwandfrei funktionierte oder weil der Wagen zu sehr beladen wurde.

3.4.3 Planungsfehler

- Zeitplan

  Die Komplexität und Größe des Projektes wurden von Anfang an unterschätzt, die Planungsphasen waren nicht realistisch, das Gesamtprojekt konnte also garnicht im Rahmen fertiggestellt werden. Durch sorgfältige Prüfung hätte dieses Problem bemerkt werden und die Planung neu konzipiert werden müssen. Außerdem waren die Phasen nicht gut aufeinander abgestimmt. Die Planung des Gepäcksystems begann zwei Jahre später als der Bau der Gebäude, die Tunnel die von diesem System benutzt werden sollten waren zu diesem Zeitpunkt bereits gebaut, waren aber für ein Gepäcksystem zu klein. Die BAE nahm den Antrag im Wissen an, den Zeitplan von zwei Jahren nicht einhalten zu können. Die Konzeption und der Bau des Gepäcksystems waren eigentlich ein Drei- bis Vierjahreprojekt, sollten aber innerhalb von zwei Jahren fertig gestellt werden.

- Testphase

  Für eine ausführliche Testphase wurde keine Zeit eingeräumt. Vor der Vorführung des Systems vor den Medienvertretern war es nicht zum Laufen gebracht worden. Z.B. am Münchner Franz-Josef-Strauß-Flughafen, wo eine kleineres aber ähnliches Gepäcksystem eingebaut wurden, wurde das System vor Inbetriebnahme zwei Jahre lang getestet, davon lief es während des letzten halben Jahres 24 Stunden am Tag.

- Modifikationen

  Wegen anhaltender Probleme kam es zu vielen Änderungen und Neugestaltungen des Systems. Dadurch wuchs die Komplexität schnell an, durch Kommunikationsprobleme zwischen BAE und Generalbauleitung wurden Modifikationswünsche zu spät weitergegeben und erschwerten den reibungslosen Ablauf des Projekts.

- Mitarbeiterschulungen

  Mitarbeiter wurden zum Teil nicht genug geschult. So kam es z.B. zu Problemen, weil die Koffer aufrecht auf das Fließband gestellt wurden. Wurden sie flach hingelegt, ging kein Koffer verloren.

3.5 Maßnahmen zur Verhinderung

Das Unglück hätte eventuell verhindert werden können, wenn einige wichtige Punkte beachtet worden wären.

- Bei einem innovativen und für die Beteiligten neuartigem Projekt sollte von den Erfahrungen von Experten profitiert werden. In diesem Fall

hätten die Erfahrungen anderen Flughäfen mit ähnlichen Systemen einbezogen werden können. Doch auch zur Projektorganisation hätten Ratschläge eingeholt und Kritiken ernst genommen werden müssen. Das Consulting-Büro Brieier Neidle Patron and Associates warnte z.B. vor dem Bau des vollautomatische Gepäcksystem, da der Projektplan keine Zeit für einen solchen Technologiesprung einräumte, was jedoch von seiten der Bauleitung nicht weiter beachtet wurde.

- Die Testzeit war nicht ausreichend, der Eröffnungstermin musste immer wieder verschoben werden, da ständig gravierende Fehler bei den Tests auftraten. Der erste Problelauf vor einer Gruppe von Medienvertretern hätte besser vorbereitet sein müssen.

- Die Fehlertoleranz des Systems war viel zu niedrig, es wurde kein Spielraum für Fehler eingeräumt. Das Gepäcksystem funktionierte nur dann einwandfrei, wenn alle Komponenten auf höchstem zu erwartenden Niveau arbeiteten.

4 Besondere Anforderungen logistischer Problemstellungen

4.1 Komplexität

Logistische Probleme sind im Allgemeinen sehr komplex, viele kleine Einheiten eines Systems müssen koordiniert werden. Dadurch wird das jeweilige System, aber vor allem auch die Software die es steuern soll, sehr unüberschaubar. Nicht alle Zustände des Systems können vorher berechnet oder getestet werden, deshalb sind lange und sorgfältig geplante Testphasen des fertigen Systems um so wichtiger. Eigentlich kleine oder unwichtig erscheinende Fehler können durch die enorme Komplexität eskalieren und zu Katastrophen führen.

4.2 Politik

Da es sich bei den angesprochenen logistischen Systeme oft um sehr groß Projekte handelt und diese oft in öffentlichen Einrichtungen genutzt werden sollen, kommen Einflußgrößen wie politische Parteien, lobbyistische Gruppen usw. hinzu. Bei Entscheidungen spielen oft viel Geld, Ansehen einzelner Personen oder der Imagegewinn durch das Projekt eine Rolle. Dabei ist es wichtig, dass Entscheidungen nicht aus taktischen Überlegungen heraus, sondern möglichst objektiv zum Wohle des Projekts gefällt werden.

4.3 Projektmanagement

Vernünftiges Projektmanagement sollte mit den Anforderungen wie Zeitdruck, beschränkte finanzielle Mittel, usw. umgehen können und eventuell Abstriche im Leistungsumfang oder der Bauzeit in Kauf nehmen. Die vielen Akteure eines großen Projekt müssen unter einen Hut gebracht werden, die Kommunikation ist sehr wichtig. Auch das Einbeziehen von Mitarbeitern in den Entstehungsprozess kann von großem Vorteil sein, bei Projektende muss die Mitarbeiterschulung eingeplant werden.

5 Resümme

Beide vorgestellten Probleme beruhten nicht auf einem verheerenden Fehler im System, sondern auf vielen, meist kleinen, Fehlern. Diese wurden entweder garnicht entdeckt (wegen fehlender Tests), unterschätzt oder schlichtweg ignoriert (oft aus politischem- oder Leistungsdruck). Das größte Problem bei logistischen Softwarelösungen ist die Komplexität und die damit verbunden unvorhersagbare Reaktion auf Fehler im System. Neben sorgfältigen Tests kann das Profitieren von Erfahrungen anderen eine große Hilfe sein. Fehler im Bereich der Logistik können, wie in den beiden vorgestellten Fällen sehr große Schäden anrichten, da oft viel Geld im Spiel ist, das Interesse der Öffentlichkeit, vor allem an innovativen Projekten, sehr groß ist und sogar Menschenleben gefährdet werden können.

Literatur

[1] Finkelstein, Anthony & Dowell, John: ≪A Comedy of Errors: the London Ambulance Service case study≫
School of Informatics, City University, UK

[2] Finkelstein, Anthony (1993): ≪Report of the Inquiry Into The London Ambulance Service≫*International Workshop on Software Specification and Design Case Study, University College London)*
http://www.cs.ucl.ac.uk/staff/A.Finkelstein/las/lascase0.9.pdf

[3] ≪The risk digest - Forum on Risks to the Public in Computers and Related Systems≫
http://128.240.150.127/Risks/13.88.html

[4] Montealegre, Ramiro: ≪What Can We Learn from the Implementation of the Automated Baggage-Handling System at the Denver International Airport?≫*Univerity of Colorado, Boulder*
http://hsb.baylor.edu/ramsower/ais.ac.96/papers/monteal.htm

[5] Schloh, Michael: ≪Analysis of the Denver International Airport baggage system≫
http://www.csc.calpoly.edu/ dstearns/SchlohProject/csc463.html

[6] Eipe, Rohit: ≪The importance of software architecture: Denver International Airport's automated baggage handling system≫
http://wiki.cs.uiuc.edu/cs427/Essay+by+Rohit+Eipe%3A+Denver+Intnl+Airport%3A+Baggage+System

[7] DIA Automated Baggage Handing System
http://www.csc.calpoly.edu/ dstearns/SchlohProject/reasons.html