Internet Science – High Reliability or When Things go wrong and as things change

Tilman Eberspächer
Betreuer: Heiko Niedermayer
Seminar Future Internet SS 2014
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
eberspae@in.tum.de

KURZFASSUNG

Fehler passieren jeden Tag und überall. Gründe hierfür sind menschliches Fehlverhalten, maschinelle Ausfälle, fehlerhafte Arbeitsabläufe, mangelnde Kommunikation und viele mehr. In seinem Buch „Friendly Fire“ analysiert Scott A. Snook welches Fehlverhalten und welche Rahmenbedingungen am 14. April 1994 zum Abschuss zweier Transporthubschrauber vom Typ UH-60 Black Hawk durch zwei U.S. Air Force F-15 Kampfflugzeuge im Luftraum über dem nördlichen Irak führten, trotz AWACS-Luftüberwachung dieses Areals. Seine Analysen werden in dem vorliegenden Text zusammengefasst um anschließend Parallelen für die Bedeutung und Vermeidung von Fehlern in Informationstechnischen Arbeitsabläufen und Projektumsetzungen zu ziehen.

1. Einleitung

Die Lebensdauer von Software verlängert sich immer weiter. Fehler innerhalb einer Software zu beheben, wird mit zunehmendem Alter der Software immer schwerer, zeitaufwändiger und damit teurer. Fehler innerhalb kritischer Systeme, wie beispielsweise Flugcomputer oder medizinischer Geräte können neben finanziellem Schaden erheblichen gesundheitlichen Schaden bei Menschen verursachen. Nicht immer sind die Gründe für Unfälle oder Ausfälle offensichtlich. Selbst wenn die Ursachen für Fehler auf den ersten Blick eindeutig scheinen, lohnt sich doch eine genaue Analyse der Umstände in dem der jeweilige Fehler aufgetreten ist. Um dies hervorzuheben, wird in den folgenden Kapiteln der Abschuss zweier U.S. Army Hubschrauber durch sogenanntes „Friendly Fire“, also durch die eigenen Verbündeten, betrachtet. Bei diesem Abschuss starben alle 26 Insassen der beiden Hubschrauber.

Die Umstände, die zu diesem Abschuss führten, erläutert Scott A. Snook in seinem Buch „Friendly Fire“. Snook selbst hegt großes Interesse an diesem Vorfall, aufgrund einer erhaltenen Verletzung im Zuge seines Militärdienstes durch Friendly Fire. Obwohl der Vorfall, wie sich zeigen wird, großteils nicht durch technisches Versagen oder Softwarefehler ausgelöst wurde, gibt Snooks Analyse doch tiefe Einblicke in die Natur von Fehlern und deren Auftreten bei dem Zusammenspiel verschiedener Akteure. Die Tatsache, dass trotz umfassender und erschöpfender Untersuchungen keinem der Beteiligten die alleinige oder ein Großteil der Schuld an dem Vorfall gegeben werden konnte, gestaltet den Vorfall umso interessanter.

Bei der Analyse der Geschehnisse betrachtet Snook nicht nur die Rollen der unmittelbar Beteiligten, sondern zieht ebenfalls einen weiten Bogen über den Kontext des Vorfalls, sowohl in historisch-politischen Belangen als auch in Hinblick auf strukturelle Faktoren innerhalb des amerikanischen Militärs, die den Vorfall begünstigten. Dieser Text beschränkt sich bei der Beschreibung der verwendeten Militärtechnik sowie der Organisationsstrukturen auf das Minimum um den Vorfall angemessen zu beschreiben. Um die Geschehnisse zur Gänze nachvollziehen zu können, ist es ratsam das Buch zur Lektüre heranzuziehen. Es bietet einen tiefen Einblick in die Entwicklung von Organisationen über einen langen Zeitraum.

Der vorliegende Text betrachtet zunächst in Kürze was passierte. Anschließend wird für die betreffenden Beteiligten betrachtet, warum sie sich so verhielten um zu beschreiben wie der Vorfall passieren konnte. Im Zuge dessen werden für die jeweiligen erkennbaren Fehler Parallelen zu Softwareentwicklung gezogen.

2. Was ist passiert?

Kurz vor Ende des zweiten Golfkrieges, am 7. April 1991, starteten die Vereinigten Staaten „Operation Provide Comfort“ (OPC). Ziel dieser Unternehmung war die Sicherung des Nord-Irak. Dies umfasste den Schutz von Neuansiedlungen kurdischer Flüchtlinge sowie das Durchsetzen der Flugverbotszonen und das Unterdrücken erneuter Aufstände; kurz: die Gewährleistung von Recht und Ordnung. OPC war als „Combined Task Force“ (CTF) konzipiert. Das bedeutet nicht nur verschiedene Einheiten des amerikanischen Militärs, sondern auch verschiedene Einheiten anderer Nationen waren an der Umsetzung beteiligt.

Um in dieser Zusammenstellung zwischen befreundeten und feindlichen Fluggeräten zu unterscheiden, wurde ein „Identification Friend or Foe“ (IFF) System eingesetzt. Dieses besteht aus zwei Komponenten: Einem „Interrogator“ und einem „Transponder“. Jedes Fluggerät trägt einen Transponder. Wenn dieser von einem Interrogator auf der richtigen Frequenz angesprochen wurde, antwortete dieser mit einem numerischen Puls. Es handelt sich hierbei also um ein Challenge-Response-Verfahren. Die Werte der erwarteten Antworten werden über kryptographische Schlüssel festgelegt. Es gibt fünf verschiedene Modi die abgefragt werden können. Modus IV und V sind für die Benutzung von NATO-Streitkräften vorgesehen. Auf die Rolle des IFF im Zusammenhang mit

doi: 10.2313/NET-2014-08-1_07

dem hier beschriebenen Unfall wird in den Abschnitten 3.1 und 3.2 genauer eingegangen.

Am 14. April 1994 gab es drei direkt beteiligte Mitspieler an dem betrachteten Vorfall, auf die sich diese Zusammenfassung konzentriert: Die beiden Black Hawk Hubschrauber, Typ UH-60, der U.S. Army, die Besatzung des E-3B Airborne Warning and Control System (AWACS) und die beiden Piloten der F-15 Eagle Fighter. Sowohl AWACS als auch die F-15 waren Teil der U.S. Air Force. Das AWACS ist eine modifizierte Boeing 707, ausgerüstet mit Systemen zur Überwachung, Kommunikation und vielfältigen Sensoren um diese Aufgaben zu erfüllen. Vereinfachend kann es als fliegender Kontrollturm betrachtet werden. Es verfügt über eine konstant bestehende Leitung zum Bodenkommando.

Am 14. April 1994 startete das AWACS um 0736. Nach Erreichen einer Höhe von 32.000 Fuß, etwa 9.750m, wurden die Systeme gestartet. Dies dauert für gewöhnlich etwa 30 Minuten. Anschließend begab sich AWACS in sein Zielgebiet um den dortigen Luftverkehr zu überwachen. Alle Systeme waren einsatzbereit und es gab keine erkennbaren Probleme.

Die beiden Black Hawks, genannt Eagle 01 und Eagle 02, starteten um 0822. Um 0935 meldeten sie sich bei AWACS an, um in die Flugverbotszone einzutreten. Um 0941 landeten sie in Zakhu um ihre Passagiere aufzunehmen, von wo sie um 0954 wieder starteten und den Start wiederum an AWACS meldeten. Auf dem Rückflug, etwa um 1011, flogen sie in ein tiefes Tal und verschwanden von den Überwachungsmonitoren des AWACS.

Die beiden F-15, genannt Tiger 01 und Tiger 02, erhielten ihr Briefing um 0735 und starteten ihre Maschinen um exakt 0900. Ihre Mission war die Säuberung des Areals von allen feindlichen Flugzeugen und Helikoptern. Nach den routinemäßigen Checks starteten sie um 0935. Sie traten um 1020 in die „Tactical Area of Responsibility“ (TAOR) ein. Zwei Minuten später meldete Tiger 01 Radarkontakt mit einem niedrig und langsam fliegenden Fluggerät 40 Meilen südöstlich seiner Position. Nachdem AWACS keinen Radarkontakt bestätigen konnte, versuchten sowohl Tiger 01 als auch Tiger 02 erfolglos das Fluggerät mit ihrem IFF-Interrogator zu identifizieren. Anschließend starteten sie zur weiteren Untersuchung die Verfolgung. Die nächste Meldung bezüglich Radarkontakts seitens Tiger 01 wurde von AWACS bestätigt. Dem Protokoll folgend führten Tiger 01 und Tiger 02 eine visuelle Zielbestätigung durch. Etwa fünf nautische Meilen vom Ziel entfernt, identifizierte Tiger 01 einen sowjetischen Kampfhubschrauber. AWACS bestätigte die Meldung mit „Copy, Hinds“.

Etwa um 1030 wurden die beiden Hubschrauber, fälschlicherweise als sowjetische Kampfhubschrauber identifiziert, von je einer Rakete getroffen und explodierten. Alle Insassen waren sofort tot. Die Raketen wurden von Tiger 01 und Tiger 02 abgefeuert, nachdem sie eine falsch-negative IFF-Auswertung erhalten hatten und eine fälschliche visuelle Identifikation der Ziele durchgeführt hatten. AWACS, das zuvor mit den beiden UH-60 Helikoptern kommuniziert hatte, hatte nicht interveniert.

3. Wie konnte es passieren?

Im Folgenden wird darauf eingegangen, wie der Abschuss passieren konnte und warum die Schuldigen nicht so einfach zu finden sind, wie es die kurze Zusammenfassung im zweiten Abschnitt dieses Textes vermuten lässt. Hierfür werden für jeden der drei Mitspieler die vorherrschenden Rahmenbedingungen beschrieben und versucht ein Einblick in die jeweils befolgten Routinen zu geben. Anhand jedes Mitspielers und der spezifischen Fehler wird versucht Parallelen zu Fehlerszenarien in der Softwareentwicklung oder beim Umgang mit informationstechnischen Systemen aufzuzeigen. Die Beispiele sind zu diesem Zweck bewusst generell gehalten um die Tragweite nicht anhand von Einzelfällen zu schmälern. Neben den drei bereits genannten Akteuren, wird im Abschnitt 3.4 auf eine Entwicklung innerhalb von großen Organisationen eingegangen, die Snook als „Practical Drift“ bezeichnet.

3.1. UH-60 Black Hawks / Eagle 01 und Eagle 02

Seitens der beiden Helikopter können zwei technische Aspekte genannt werden: Zum einen die technische Fehlfunktion des IFF, wobei diesbezüglich trotz ausführlicher Untersuchungen nicht endgültig geklärt werden konnte, ob der Transponder der Black Hawks oder der Interrogator der F-15 nicht korrekt funktionierte. Zum anderen die technisch mangelhafte Ausstattung in Bezug auf das verwendete Kommunikationssystem.

Das IFF-System wurde von Tiger 01 auf zwei Kanälen abgefragt, nachdem Eagle 01 und Eagle 02 als Radarkontakte erkannt wurden: Zunächst wurde eine Challenge auf Mode I CC gesendet. Mode I war hierbei der generelle Code, mit dem jedes Fluggerät der Koalition antworten sollte innerhalb der TAOR. „CC“ bedeutet hierbei „Correct Code“, also der Code, der für diesen Tag laut Briefing festgesetzt war. Als keine positive Antwort erhalten wurde, änderte Tiger 01 den Modus auf „Auto“. In diesem Modus sendet der IFF-Interrogator kontinuierlich Challenges auf Mode IV. Mode IV war der zweite Modus, auf dem jedes Fluggerät der Koalition antworten sollte. Auch hier erhielt Tiger 01 keine Antwort. Auf zwei verschiedene Challenges erhielt Tiger 01 also jeweils keine Antworten [1]. Diese nicht vorhandenen Antworten können als Falsch-negativ betrachtet werden.

Sowohl AWACS als auch Tiger 01 und Tiger 02 waren ausgestattet mit einem damals unterbrechungssicheren Kommunikationssystem, dem „HAVE QUICK“, auf dessen Gebrauch sie innerhalb der TAOR umschalteten. Es umgeht Versuche die Kommunikation zu stören durch Frequenz-hopping, also das schnelle Wechseln zwischen verschiedenen Frequenzen anhand eines bestimmten Musters, wodurch es gegen Störsignale auf einzelnen Frequenzen nahezu immun ist. Eagle 01 und Eagle 02 waren nicht mit dieser fortschrittlichen Technologie ausgestattet, wodurch sie nicht in die Kommunikation innerhalb der TAOR zwischen Tiger 01, Tiger 02 und AWACS eingebunden waren. Sie verfügten lediglich über Standardsysteme, deren Empfang stark von ungestörten Sichtverhältnissen abhängt. Diese waren nicht gegeben, nachdem Eagle 01 und Eagle 02, den Standardprozeduren folgend, in das Tal eingetreten waren. So verschwanden die

beiden Helikopter nicht nur von dem Radar des AWACS, sondern konnten auch nicht mehr Kommunizieren.

Solche Fehler treten in verteilt entwickelten Systemen oder verteilt arbeitenden Entwicklergruppen auf. Obwohl die Möglichkeit zur sicheren oder effizienten Kommunikation innerhalb des Gesamtsystems gegeben ist, wird sie von einzelnen Teilsystemen aufgrund falscher Anforderungsspezifikation nicht oder nur teilweise genutzt. Wird nun dieser spezielle Fehlerfall von den übrigen Systemen nicht explizit geprüft, geht die Kommunikation innerhalb des Gesamtsystems verloren und das gesamte System gerät in einen instabilen Zustand. Auf Entwicklungsebene passierte genau dieses bei der Entwicklung des „Virtual Case File“, einer Applikation die für das amerikanische FBI zwischen 2000 und 2005 entwickelt werden sollte: Aufgrund schlechter Anforderungsspezifikationen und verteilter Entwicklung standen verschiedene Entwicklerteams teilweise in Konkurrenz zueinander. Es mangelte an klarer Kommunikation zwischen den Unterorganisationen und das Projekt wurde schlussendlich eingestellt [2].

Um einen sicheren und stabilen Betrieb eines Systems zu gewährleisten, ist es also notwendig für jedes Teilsystem geltende Standards zu definieren bezüglich ihrer Schnittstellen mit anderen Systemen. Dabei ist es notwendig nicht nur die Nachbarsysteme zu betrachten, mit denen interagiert wird, sondern ebenfalls einen gelten Status Quo in dem Gesamtsystem zu gewährleisten. Mit einem solchen Vorgehen können auch Ausfälle oder Fehlfunktionen einzelner Untersysteme erkannt und zu einem gewissen Grad kompensiert werden, beispielsweise bei einem byzantinischen Fehler. Ein byzantinischer Fehler beschreibt eine Fehlerklasse in einem System mit mehreren Prozessoren. Spezifisch für diese Fehlerklasse sind unterschiedliche Resultate einer Komponente, abhängig davon auf welchem Prozessor sie arbeitet [3].

Ebenfalls kann so sichergestellt werden, dass bei Erweiterungen oder Änderungen, dieses Subsystem auch von anderen Teilen über einen bestimmten Standard Daten austauschen kann. Hierfür muss für jedes Teilsystem etwaige benötigte Technik zur Verfügung gestellt werden. Ebenso ist es notwendig Kontrollmechanismen zu etablieren, um zu vermeiden, dass verschiedene Systeme auf gleichen Ressourcen arbeiten ohne den Status der anderen Beteiligten zu kennen, falls dieser systemkritisch sein kann.

3.2.F-15 / Tiger 01 und Tiger 02

Bevor auf die begangenen Fehler seitens der beiden F-15 Piloten eingegangen wird, muss deutlich gemacht werden, dass es sich bei diesen beiden Personen um erfahrene Flieger handelte. Beide hatten mehrere tausend Stunden Flugerfahrung, waren ausgeruht und hielten sich ihrem Verständnis nach präzise an die geltenden Prozeduren. Obwohl sie in letzter Instanz den Abschuss auslösten, kann ihnen, wie im Folgenden versucht wird darzulegen, nur eine Teilschuld eingeräumt werden. Die Fehlfunktion des IFF wurde bereits im vorhergehenden Abschnitt näher erläutert, deshalb wird hier darauf verzichtet um Redundanz zu vermeiden.

Aufgrund der negativen IFF-Überprüfung unternahmen Tiger 01 und Tiger 02 eine visuelle Bestätigung des Ziels. Dies ist notwendig, da eine IFF-Challenge nur bestätigen kann, dass es sich bei dem Ziel um ein befreundetes Flugobjekt handelt. Fällt die Abfrage negativ aus, deutet dies jedoch nicht notwendigerweise auf ein feindliches Flugobjekt hin. Tiger 01 sagte im Zuge der Untersuchung des Vorfalls aus, dass nach dem Wechsel der IFF-Einstellung von Mode I CC auf Mode IV kurzzeitig ein verbündetes Flugobjekt an der Position von Eagle 01 und Eagle 02 angezeigt wurde. Diese Anzeige verschwand allerdings kurz nach dem Umschalten wieder. Nach Aussage des Piloten war dies ein häufiger auftretendes Verhalten des IFF in den geflogenen Jets, welches er schon im Verlauf anderer Missionen beobachtet hatte. Deshalb trat keine Verwunderung seinerseits auf [4]. Als Tiger 01 an den Helikoptern vorbeifliegt, ist er etwa 150 Meter über und 300 Meter seitlich von ihnen. Er fliegt in etwa mit einer Geschwindigkeit von 830 km/h. Snook zieht den folgenden Vergleich, um die Größenordnungen und Relationen zu verdeutlichen:

„Imagine trying to tell the difference between a Chrysler Caravan and a Ford Aerostar minivan as one of them passed by you going the other direction […] and each of you is driving 150 miles per hour, and your two lanes were separated by at least three football fields, and the only view you had of the vans was from above and behind, and the vans were painted with appropriate camouflage paint, and you suspect that the passengers in the vans might be armed with the intent of shooting at you after you passed them, and you had a mountain staring you in the face, and you had to make this call while your boss observed your performance from another car driving behind you.“[5]

Dieses Zitat zeigt die wesentlichen Punkte, die zu der fehlerhaften Identifikation führten. Abgesehen von der Distanz und der hohen Geschwindigkeit war der Blickwinkel suboptimal für die Unterscheidung zwischen den beiden Helikoptertypen. Hinzu kommt die Ausstattung der Black Hawks an diesem Tag mit zusätzlichen Treibstofftanks unterhalb der Pontons (der „Flügel“), die die Ähnlichkeit mit dem von Tiger 01 erkannten Modell zusätzlich erhöhten.

Weiterhin war die Vorbereitung der beiden Piloten auf die visuelle Unterscheidung von Hubschraubern nicht mehr aktuell aufgrund zeitlicher Faktoren einhergehend mit den Einsatzplänen der Piloten. Einer der wichtigsten Punkte: Tiger 01 und Tiger 02 wussten nicht, dass verbündete Black Hawks an diesem Tag in der TAOR unterwegs waren. Ohne das Wissen um die Möglichkeit, dass die erkannten Fluggeräte freundlich sein könnten, erwarteten sie feindliche Helikopter. Für F-15 Piloten war es eine inoffizielle Regel, dass bei einer solchen „Säuberungsmission“ eines Areals nur das betreffende AWACS zur Überwachung vor ihnen startet. Aussagen des Piloten von Tiger 01 zufolge sah er tatsächlich den Helikoptertyp, den er angab. Diese optische Täuschung beziehungsweise Fehlinterpretation visueller Daten resultierte aus dem sehr kurzen visuellen Eindruck und seiner unterbewussten Erwartungshaltung, resultierend aus dem Missionsziel und dem unvollständigen Briefing.

Des Weiteren intervenierte AWACS nicht, als Tiger 01 die Radarkontakte meldete. Dies ist ein häufiges Phänomen in Organisationen mit klarer Hierarchie: Solange die Kontrollinstanz nicht interveniert, wird angenommen das Verhalten sei korrekt. So wurden die Piloten von Tiger 01 und Tiger 02 in ihrer Beobachtung es handle sich um feindliche Hubschrauber weiter bestärkt.

Snook spricht noch weitere Faktoren an, wie die anhaltende Rivalität zwischen F-15 und F-16. Den Piloten war bekannt, dass nach ihnen eine F-16 Patrouille das Gebiet sichern sollte. Diesen wollten sie einen sicheren Abschuss nicht überlassen. Kampfpiloten brüsten sich mit der Anzahl ihrer Abschüsse gegenüber anderen Piloten. Im Verlauf des Krieges war die Abschussquote der F-16 aufgrund ihres taktischen Einsatzzweckes höher als die der F-15. Während die F-15 eher für Kämpfe mit anderen Hochgeschwindigkeitsflugzeugen eingesetzt wurde, flogen die F-16 tiefer und hatten als Primärziel langsamere Objekte wie Hubschrauber.

Die Erwartungshaltung der Piloten, gepaart mit unzureichenden Informationen über die vorherrschenden Rahmenbedingungen und einem undeutlichen visuellen Reiz können als Hauptursache für das Verhalten der Piloten angesehen werden. Hinzu kommt das Verlangen den erwähnten F-16 zuvor zu kommen. Abbildung 1 zeigt das Zusammenspiel der einzelnen Teilfaktoren. Das Venn-Diagramm zeigt die visuelle Identifikation als Schnittmenge der drei bereits genannten Teilaspekte. Ebenso beschreibt die Abbildung Stichpunktartig die Gründe für die undeutliche visuelle Erkennung und zeigt ein weiteres Venn-Diagramm, das die Entstehung der Erwartungshaltung darstellt.

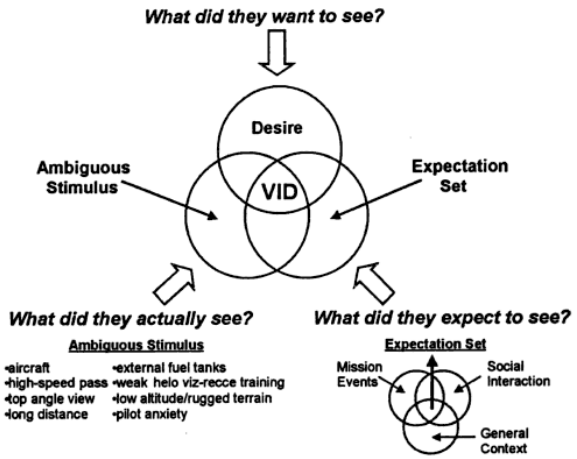

Abbildung 1: Entscheidungsfaktoren der F-15 [6]

Fehler basierend auf falschen Erwartungshaltungen sind menschlich. Da diese nie komplett ausgeschlossen werden können, ist es umso wichtiger ein Umfeld zu schaffen, in dem solche Fehler nicht zusätzlich begünstigt werden. Dazu gehört beispielsweise ausreichend Zeit um mit dem Status Quo vertraut zu werden. So können Verdachtsmomente ausgeräumt werden und fundierte Vermutungen angestellt werden. Obwohl ein Projekt oder das Beheben eines Fehlers innerhalb eines Projekts zeitkritisch ist, kann es auch in der Softwareentwicklung fatale Auswirkungen haben, eine Fehlerursache aufgrund von Vermutungen vermeintlich zu beheben ohne genau zu analysieren, ob der Fehler wirklich an dieser Stelle auftritt. Neben unnötigen Mehraufwand können so weitere Fehler in den Code eingebracht werden aufgrund unsauberen Arbeitens oder entstehender Redundanz.

Die falsche visuelle Identifikation der Ziele zeigt weiterhin die Notwendigkeit ausreichend zuverlässiger Kompensationsprozeduren bei Ausfall einer Schlüsselfunktion. Die Fehlerrate unter den gegebenen Umständen ist bei rein visueller Identifikation erwartungsgemäß viel höher als die Wahrscheinlichkeit eines Falsch-positiven oder –negativen Ergebnisses bei Abfrage mit Hilfe eines IFF-Systems. Um dies zu umgehen, kann auf den Einsatz von „fail-safe“-Systemen zurückgegriffen werden. Diese verhindern Ausfälle kritischer Komponenten zwar nicht, gewährleisten jedoch, dass im Falle eines Fehlers das System nicht weniger sicher ist, als wenn dieser Fehler nicht auftritt [7]. Ebenso zeigt die Gleichgültigkeit, mit der Tiger 01 die Fehlfunktion bei Umschaltung auf Mode IV hinnimmt, die Wichtigkeit von nachhaltiger Wartung solch kritischer Systeme.

3.3.AWACS

Während festgestellt wurde, dass Eagle 01 und Eagle 02 mit veraltetem Equipment flogen und in dem verwendeten IFF ein Fehlverhalten auftrat, muss bei der Rolle der Crew des AWACS nachgeforscht werden, warum diese nicht intervenierten, als Tiger 01 zwei unbekannte Radarkontakte meldete.

Betrachtet man die Mitglieder der AWACS-Besatzung einzeln, ist auch hier festzustellen, dass jeder von ihnen für seine Stellung hoch qualifiziert war. Jedes Mitglied verfügte über ausreichend Erfahrung auf seinem spezifischen Gebiet, war ausgeruht und voll einsatzfähig. Liegt das Augenmerk allerdings auf der Besatzung als Ganze, ist festzustellen, dass sie in dieser Zusammensetzung keinerlei Erfahrung aufweisen konnte. Jede AWACS-Besatzung muss vor einem Einsatz mindestens zwei komplette Simulationsläufe erfolgreich durchführen. Dies war jedoch nicht geschehen aufgrund verschiedener Faktoren wie Krankheit, verspätetes Eintreffen in der Operationszone, Rotationspläne der Einsatzziele und Ähnlichem. Snook unterscheidet zwischen fünf verschiedenen Graden der Performanz eines Teams [8]:

- „Working Group“: Mitglieder agieren primär um Informationen zu teilen. Davon abgesehen gibt es keine tiefer greifende Zusammenarbeit
- „Pseudo-Team“: Mitglieder versuchen zusammen zu arbeiten, dabei sinkt jedoch die Leistung jedes einzelnen Mitgliedes, sodass die Gesamtleistung niedriger als die Summe der Einzelleistungen ausfällt
- „Potential Team“: Mitglieder arbeiten teamorientiert, aber nicht optimal; die Performanz ist etwa die einer Working Group
- „Real Team“: Eingespieltes Team, Mitglieder arbeiten auf ein gemeinsames Ziel hin und fühlen sich für die Leistung der Gruppe verantwortlich
- „High Performance Team“: Erfüllt alle Kriterien des „Real Team“, Mitglieder sind darüber hinaus

an der Weiterentwicklung der übrigen Gruppenangehörigen sehr interessiert

Aufgrund des fehlenden gemeinsamen Trainings und daraus resultierender nicht existenter Erfahrung in dieser spezifischen Zusammensetzung, ist die AWACS-Besatzung an diesem Tag als „Pseudo-Team“ einzustufen. Obwohl also jedes Mitglied selbst qualifiziert genug war für die Mission, konnte die Gruppe als solche sie nicht optimal erfüllen.

Hinzu kommen Gewohnheitsfaktoren der Mitglieder: So gibt ein Mitglied bei einer Befragung zu Protokoll, er habe immer ein Buch dabei, da er nirgendwo soviel lese wie während eines Fluges. Ebenso gab es keine offiziellen Protokolle für die Behandlung von U.S. Army Flugobjekten innerhalb der TAOR seitens der U.S. Air Force AWACS. Ein Mitglied der AWACS-Besatzung gibt an, dass Angehörige der U.S. Army sich manchmal anmeldeten, wenn sie in die TAOR eintraten, es manchmal aber auch unterließen. Daraus resultierend gab es keine feste Vorgehensweise bezüglich der Behandlung der Hubschrauber innerhalb der TAOR. Somit fühlte sich keines der Mitglieder der Besatzung dafür zuständig, Tiger 01 und Tiger 02 über die Anwesenheit der Hubschrauber aufzuklären.

Dies wird besonders dadurch deutlich, dass nach Abbruch des Radarkontakts zwischen Eagle und AWACS bei Eintritt in die Berge zwar ein Marker seitens der Besatzung gesetzt wurde, der die letzte Position auf dem Radar anzeigt, dieser aber nach 60 Sekunden verschwand weil sich niemand dessen annahm. Ähnlich wie Tiger 01 und Tiger 02 verließ sich unterbewusst jedes der Mitglieder darauf, dass sein jeweiliges Kontrollorgan auf Fehler aufmerksam machen würde.

Es kommt weiterhin erschwerend dazu, dass die Stellung der Besatzung innerhalb der Air-Force nicht die beste ist. Obwohl die Befehlshierarchie darlegt, dass die Besatzung als Kontrollorgan theoretisch einen signifikanten Einfluss auf die Aktionen von Kampfpiloten hat, zeigt die Realität, wie Snook beschreibt, ein anderes Bild. Entgegen der theoretischen Einbindung in die Befehlsstrukturen, betrachten Kampfpiloten jede andere Klasse von Angehörigen der Air-Force als minderwertig oder Piloten zweiter Klasse. So gibt ein Angehöriger der AWACS-Besatzung zu Protokoll, dass er für gewöhnlich in die Entscheidungen, die ein Kampfpilot trifft, nicht eingreift, da diese Einmischung ohnehin meist ignoriert wird [9]. In Anbetracht dieser gesellschaftlichen Strukturen ist es nicht weiter verwunderlich, unter Mitberücksichtigung der bereits genannten Gründe, dass niemand innerhalb der AWACS-Besatzung intervenierte oder sich dazu berufen oder verpflichtet fühlte, in irgendeiner Art und Weise der visuellen Bestätigung durch die Kampfpiloten Tiger 01 und Tiger 02 zu widersprechen.

Es bleibt also festzuhalten, dass die AWACS-Besatzung zwar versäumte zu intervenieren und dadurch ein tragischer Unfall begünstigt wurde. Dennoch muss beachtet werden, dass aufgrund fehlender Ablaufprotokolle seitens der Einbindung von U.S. Army Operationen in U.S. Air Force Operationen kein Mitglied der Besatzung voll dafür verantwortlich gemacht werden kann. Weiterhin wurde durch die gesellschaftliche Struktur innerhalb der Air-Force die nicht-Einmischung seitens der Besatzung gerechtfertigt.

Solche Fehler sind typisch bei großen Softwareprojekten. Es ist gängige Praxis knappe Zeitpläne durch erhöhte Entwicklerzahlen zu kompensieren. An dieser Stelle schlägt jedoch direkt die Auswirkung des „Pseudo-Teams“ zu: Anstatt die Performanz der Gruppe zu erhöhen, werden bereits etablierte Entwickler in ihrer Arbeit verlangsamt durch Einarbeitung der neuen Kollegen. Nicht selten werden Entwickler hierfür von ihrer eigentlichen Aufgabe abgezogen und als Leiter kleinerer Sub-Teams eingesetzt. Mit dieser neuen Rolle sind sie nicht vertraut und begehen Fehler, die vermeidbar wären. Die neuen Kollegen wiederum brauchen Zeit um sich in die Unternehmensstrukturen, die Programmierrichtlinien und das neue soziale Umfeld einzufinden. Die jeweiligen Zuständigkeiten sind nicht mehr klar gegliedert und undurchsichtiger, je größer das jeweilige Softwareprojekt ausfällt. Dies erhöht signifikant die Fehlerquoten durch Einbindungskonflikte, Programmierstile und mangelnde Kenntnis der Projektumgebung, sowie mangelnde Identifikation mit den Zuständigkeiten und Verantwortlichkeiten der individuell eingenommenen Rolle [10].

Dasselbe Phänomen ist nicht nur bei dem Einsatz externer Entwickler, sondern ebenfalls bei ad hoc rekrutierten Testern zu beobachten. Sie sind nicht vertraut mit Testprotokollen, legen unterschiedlichen Wert auf exploratives Testen und sind andere Aktionsabläufe beim Finden von Fehlern gewohnt. Im schlimmsten Falle sind die Tester selbst unerfahren, da übersehen wird, dass effektives und effizientes Testen Fähigkeiten sind, die es zuerst zu erlernen gilt, bevor sie umgesetzt werden können [11]. Dies zeigen auch die Ergebnisse diverser Studien bezüglich der Erfolgsfaktoren im Projektmanagement und somit auch im Management von IT-Projekten. Die drei wichtigsten Faktoren hierbei sind Kommunikation, Zieldefinition und Qualifikation der Mitarbeiter [10].

3.4.Practical Drift

Um die dynamische Natur der Zusammenhänge zwischen Unterorganisationen in einem größeren Kontext zu erklären, führt Snook eine Theorie ein, die er als „Practical Drift“ bezeichnet. Kurz gefasst besagt er in dieser Theorie, dass Angehörige einer Organisation immer einen billigeren, einfacheren oder effizienteren Weg finden werden Aufgaben zu erledigen und deshalb von vorgegebenen Richtlinien oder Prozessen abweichen werden. Im Zuge dieses Vorganges stabilisiert sich ein momentan instabiles System aus Aktionsmotiven und Organisationsbindungen selbst. Er bezeichnet dieses Verhalten kurz als „[…] the slow steady uncoupling of practice from written procedure“ [12]. Dies führt dazu, dass Vorgehensweisen, die sich lokal als effektiv und effizient erweisen, durch Wiederholung legitimiert werden. Es ist eine direkte Folge aus dem Umstand, dass aufgestellte Regeln nicht immer direkt auf die vorherrschende Situation anwendbar sind oder in dieser spezifischen Situation suboptimal erscheinen. Dies liegt zumeist an einer Überdefinition der Regeln.

Kommt nun zu diesem Phänomen des „Practical Drift“ eine plötzliche enge Bindung zwischen verschiedenen Unterorganisationen, die im Laufe der Zeit ihre eigenen

Versionen der Prozesse und Richtlinien durch Wiederholung etabliert haben, entsteht ein gefährliches Moment, welches Snook als weitere Ursache für den Abschuss der beiden UH-60 Black Hawk Helikopter angibt. Dies ist einer der besagten instabilen Momente innerhalb eines Systems.

Hätten alle Beteiligten die gleiche Auffassung der Prozesse gehabt, wäre der Vorfall wahrscheinlich nicht eingetreten. Hätten sich die Helikopter der U.S. Army bei jedem Flug bei AWACS an- und abgemeldet, wäre schnell aufgefallen, dass es seitens der Army nicht klar war, dass innerhalb der TAOR geänderte IFF-Codes genutzt wurden und dieser Umstand hätte behoben werden können. Ebenso wären die möglichen Auswirkungen des teilweisen Einsatzes veralteter Technik innerhalb der Black Hawk Helikopter wahrscheinlich eingehender betrachtet worden. Wäre die Army korrekt und umfassend in die Verlaufspläne der Air Force eingebunden gewesen, hätten Tiger 01 und Tiger 02 innerhalb ihres Briefings die Information erhalten, dass an diesem Tag vor ihrem eigenen Start bereits zwei Helikopter gestartet waren.

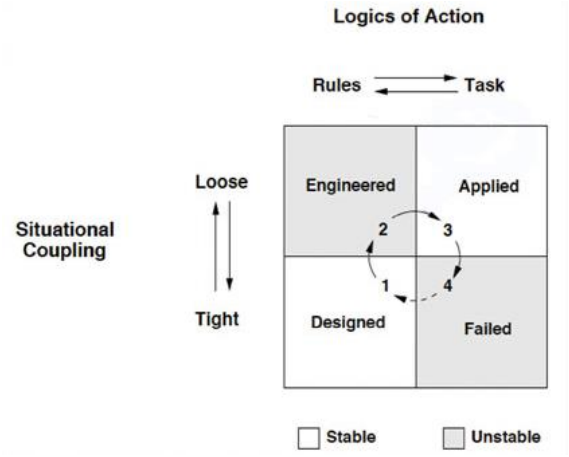

Abbildung 2: Practical Drift [13]

Abbildung 2 zeigt Snooks Modell in drei Dimensionen: Aktionslogik, situationelle Verbundenheit und Zeit. Aktionslogik kann entweder auf Regeln oder die zu bewältigende Aufgabe ausgelegt sein. Die situationelle Verbundenheit ist entweder eng oder lose. Die Zeit wird anhand der Zahlen 1 – 4 dargestellt. Quadranten 1 und 3 kennzeichnen hier stabile Zustände, die Aktionslogik passt zur vorherrschenden Situation. In den Quadranten 2 und 4 ist das System instabil, lose Bindungen sind nicht vereinbar mit regelbasierten Aktionen, ebenso wenig wie enge Bindungen mit aufgabengetriebenen Aktionen.

Was das bedeutet, erklärt folgendes Beispiel: Um den Prozess der Softwareentwicklung zu optimieren, soll ein neuer Deployment-Prozess entwickelt werden. Um nicht für vage Formulierungen zur Verantwortung gezogen werden zu können, definiert der Ersteller dieses Prozesses alles so präzise wie möglich und orientiert sich bei der Erstellung an diversen Worst-Case-Szenarien. Dadurch wird der Prozess für die praktische Umsetzung übertrieben präzise definiert. Dies ist der erste Quadrant, die Regeln sind streng definiert, die Teilprozesse eng gekoppelt.

Als der Prozess fertiggestellt ist und in den ersten Projekten eingesetzt wird, geht er in den zweiten Quadranten über. Das Vorgehen ist nach wie vor regelorientiert, aber die einzelnen Prozessgruppen sind nicht mehr so eng gekoppelt wie in der Theorie gedacht. Dieser Zustand ist instabil und geht daher langsam in den dritten Quadranten über: Im Laufe der Zeit werden für die Anwender hinderliche Teile von ihnen weggelassen oder für ihre Zwecke optimiert. Dieser Zustand ist wiederum stabil und kann über Jahre andauern. Wie Snook beschreibt, werden die angepassten Teilprozesse innerhalb der Unterorganisationen die neuen Standards.

Diese Situation bleibt jedoch nur solange stabil, bis etwas passiert, das Unterorganisationen dazu zwingt, eng miteinander zusammen zu arbeiten. In dem genannten Beispiel könnte es sich hierbei etwa um einen Fehler bei der Einbindung automatisierter Tests in den Deployment-Prozess handeln. Müssen nun zwei Unterorganisationen miteinander zeitkritisch arbeiten, während jede im Laufe der Jahre ihre eigenen Prozesse etabliert hat, ist es wahrscheinlich, dass irgendein größerer Fehler auftritt. Das System befindet sich nun im vierten Quadranten. Um das Wiedereintreten solcher Fehler zu vermeiden, werden nun neue Prozesse aufgesetzt, das System stabilisiert sich wieder in Quadrant eins. Wurden aus der Vergangenheit keine Lehren bezüglich der Etablierung von Richtlinien gezogen, beginnt der Kreislauf nun wieder von Neuem mit den neu eingeführten Regeln.

Dieses Beispiel, basierend auf Snooks Theorie, lässt folgende Schlussfolgerungen zu:

- Was Snook als „Practical Drift“ bezeichnet, ist unvermeidlich, der Mensch versucht seine Arbeit zu optimieren
- Mehr oder umfangreichere Regeln und Prozesse begünstigen dieses Verhalten
- Im Idealfall sollte der einfachste Weg etwas zu tun der richtige Weg sein
- Prozesse müssen zusammen mit denjenigen entwickelt werden, die sie später befolgen sollen
- Prozesse und Richtlinien müssen sich im Laufe der Zeit mit der gängigen Praxis ändern

Dieses Verhalten kann in jeder Organisation beobachtet werden. Der IT-Sektor bildet hier keine Ausnahme. Firmeneigene Coding-Standards werden ignoriert um schnell einen Fehler zu beheben. Lokale Administratorrechte werden an nicht ausreichend qualifizierte Nutzer vergeben, um Zeit bei der Installation von Programmen zu sparen. Firmenlaptops werden mit nach Hause genommen um weiter zu arbeiten und gehen verloren oder werden gestohlen. So wurde beispielsweise Ende 2012 einem Mitarbeiter der NASA sein Laptop gestohlen. Der Rechner selbst war zwar mit einem Passwort geschützt, die Festplatte selbst war jedoch unverschlüsselt [14]. Im Grunde genommen kann für jede geltende Regel an dieser Stelle ein Verstoß gegen selbige genannt werden. Wie bereits von Snook genannt ist der Antrieb zur Dehnung oder direkten Missachtung dieser Regeln Bequemlichkeit, Zeitersparnis oder ein Kostenfaktor. Und durch lange Zeit ausbleibenden Schaden werden diese neuen Auslegungen die akzeptierten Regeln.

doi: 10.2313/NET-2014-08-1_07

4. Zusammenfassung

Abschließend ist erneut festzuhalten, dass Fehler passieren. Die hier betrachteten Fehlerklassen reichen von technischen Defekten und mangelhafter technischer Ausstattung über menschliches Versagen aufgrund unzureichender Information und daraus resultierender Erwartungshaltung bis hin zu Passivität und suboptimaler Performanz aufgrund von unerfahrenen Teams. Keine dieser Fehlerklassen kann innerhalb von komplexen Systemen, bei deren Betrieb Menschen beteiligt sind, komplett ausgeschlossen werden.

Unter dieser Prämisse ist es sinnvoll die Rahmenbedingungen anzupassen um die Wahrscheinlichkeit des Auftretens dieser Fehler zu minimieren. Wie der „Practical Drift"-Ansatz zeigt, sind starre Strukturen hierfür kontraproduktiv, da sie auf lange Sicht betrachtet lediglich das Abweichen oder Umgehen dieser Strukturen fördern. Prozesse und Richtlinien müssen analog zur Entwicklung des Umfeldes weiterentwickelt werden, um auf geänderte Umstände weiterhin anwendbar zu sein. Korrekte und ausführliche Kommunikation zwischen Unterorganisationen, handle es sich hierbei um unterschiedliche Abteilungen innerhalb eines Unternehmens oder um Unterklassen eines Softwaresystems, sind notwendig um Störungen frühzeitig zu entdecken und darauf reagieren zu können.

Das Verhalten der AWACS-Besatzung zeigt, dass streng gegliederte Hierarchien innerhalb von Organisationen ebenso Fehler begünstigen können. Durch das Verlassen auf die jeweils nächste Kontrollinstanz ohne Intervention werden Fehler hierbei zwar von allen Beteiligten wahrgenommen, jedoch von niemandem darauf reagiert, bis es schließlich zu spät ist. In System mit strengen Hierarchien ist es daher notwendig für die einzelnen Ebenen genaue Verantwortlichkeiten zu definieren, sodass zu jedem Zeitpunkt jedem Beteiligten bewusst ist, wer sich worum kümmern muss.

5. Quellen

[1] Scott A. Snook. *Friendly Fire – The accidental shootdown of U.S. Black Hawks over northern Iraq*. Fourth Printing, and first paperback printing, 2002, Princeton Paperbacks, ISBN 0-691-09518-3, S. 60

[2] Glenn A. Fine. Congressional Testimony. http://www.justice.gov/oig/testimony/0502/final.pdf, aufgerufen am 19.3.2014

[3] L. Lamport, R. Shostak, und M. Pease: *The Byzantine Generals Problem.* In: ACM Trans. Programming Languages and Systems. 4, Nr. 3, Juli 1982, S. 382-401

[4] Scott A. Snook. *Friendly Fire – The accidental shootdown of U.S. Black Hawks over northern Iraq*. Fourth Printing, and first paperback printing, 2002, Princeton Paperbacks, ISBN 0-691-09518-3, S. 60-61

[5] Scott A. Snook. *Friendly Fire – The accidental shootdown of U.S. Black Hawks over northern Iraq*. Fourth Printing, and first paperback printing, 2002, Princeton Paperbacks, ISBN 0-691-09518-3, S. 88

[6] Scott A. Snook. *Friendly Fire – The accidental shootdown of U.S. Black Hawks over northern Iraq*. Fourth Printing, and first paperback printing, 2002, Princeton Paperbacks, ISBN 0-691-09518-3, S. 97

[7] David B. Rutherford Jr., *„What do you mean – it's fail safe? Evaluating Fail-Safety in processor-based vital control systems"*, 1990 Rapid Transit Conference, http://www.billpetit.com/Papers/Petit017.pdf, aufgerufen am 23.3.2014

[8] Scott A. Snook. *Friendly Fire – The accidental shootdown of U.S. Black Hawks over northern Iraq*. Fourth Printing, and first paperback printing, 2002, Princeton Paperbacks, ISBN 0-691-09518-3, S. 106

[9] Scott A. Snook. *Friendly Fire – The accidental shootdown of U.S. Black Hawks over northern Iraq*. Fourth Printing, and first paperback printing, 2002, Princeton Paperbacks, ISBN 0-691-09518-3, S. 132

[10] C. Engel, A. Tamdjidi, N. Quadejacob. *Ergebnisse der Projektmanagement Studie 2008- Erfolg und Scheitern im Projektmanagement.* Studienergebnisse, http://www.gpm-ipma.de/fileadmin/user_upload/Know-How/Ergebnisse_Erfolg_und_Scheitern-Studie_2008.pdf, S. 8

[11] J. Vargas, J. Córdoba. *10 Best practices for an effective testing & QA implementation.* http://www.softtek.com/newsletter/item?id=16&item=77, aufgerufen am 19.3.2014

[12] Scott A. Snook. *Friendly Fire – The accidental shootdown of U.S. Black Hawks over northern Iraq*. Fourth Printing, and first paperback printing, 2002, Princeton Paperbacks, ISBN 0-691-09518-3, S. 194

[13] Scott A. Snook. *Friendly Fire – The accidental shootdown of U.S. Black Hawks over northern Iraq*. Fourth Printing, and first paperback printing, 2002, Princeton Paperbacks, ISBN 0-691-09518-3, S. 186

[14] U. Ries. *Datenleck durch Laptop-Klau bei der NASA.* http://www.heise.de/security/meldung/Datenleck-durch-Laptop-Klau-bei-der-NASA-1750677.html, aufgerufen am 19.3.2014

doi: 10.2313/NET-2014-08-1_07