# KAPITEL 1

## Ein Beispiel für eine alltägliche technische Risikoanalyse

*Peter Ladkin*

Ich beteilige mich regelmäßig an einer Mailingliste, dich sich mit computerbasierten, safety-kritischen Systemen beschäftigt. Dort wurde vor kurzem über die Gefahr diskutiert, die von der Benutzung von Mobiltelefonen auf den Tankstellenvorhöfen ausgeht.

An dieser Mailingliste beteiligen sich nicht nur einige der bekanntesten Forscher auf dem Gebiet der computergestützten Safety, sondern auch Mitentwickler des neuen Standards IEC 61508 für die Entwicklung safety-kritischer Systeme mit "programmierbaren Elektronikkomponenten". Außerdem auch Vorsitzende der britischen Health and Safety Executive (HSE), aber auch einige Kollegen aus der Energie- und Transportwirtschaft mit großem Interesse an dieser Materie.

### 1.1 Technische Risikoanalyse

Ein Großteil des Ingenieurwesens dreht sich um die Entwicklung und Analyse von Artefakten. Dazu gehört auch die Einschätzung darüber, wie sicher die Benutzung dieser Artefakte ist. Da Artefakte sowohl komplex als auch groß sein können (man muss nur mal an eine industrielles Chemiewerk oder ein Verkehrsflugzeug denken), nennt man sie oft ‚Systeme‚. Dieser Ausdruck wird normalerweise für Artefakte verwendet, in deren Verhalten Komplexität eine wichtige Rolle spielt.

Eine Safetyanalyse eines Systems oder einer Situation folgt normalerweise grob

dem folgenden Ablauf:

Wir beginnen damit die Begriffe ‚Unfall'", ‚(Unfall-) Schwere„ ‚Hazard, und ‚(Hazard-) Dauer, festzulegen. Zuerst muss definiert werden was als ‚Unfall, betrachtet wird. Für diesen Begriff existieren viele Definitionen, wie zum Beispiel [52, Eintrag für ‚Accident,], aber prinzipiell hat man die freie Wahl. Die meisten Menschen verbinden mit dem Begriff ‚Unfall, einen schweren persönlichen Schaden, einen Schaden in ihrer Umgebung oder auch eine massive Verringerung des Kontostandes. Vermutlich ist es jedoch ratsamer hier eine genauere Definition zu verwenden. Weiterhin müssen Unfälle anhand ihrer ‚Schwere, [1] klassifiziert werden. Handelt es sich um einen Kratzer oder einen Bruch? Liegen die entstandenen Kosten bei einem Dollar oder einer Millionen Dollar? Außerdem müssen ‚Hazards, identifiziert werden. Das sind Zustände, entweder des Systems, der Umgebung oder von beiden zusammen, welche Vorgänger eines Unfalls sind. Nicht jeder Hazard muss zwangsläufig zu einem Unfall führen; aber die Idee ist, dass ein Unfall durch die erfolgreiche Behandlung eines Hazards verhindert werden kann. Hazards bestehen für eine bestimmte Zeitspanne (die ‚Dauer„ [52] zitiert [44, Kapitel 9]).

An dieser Stelle hat man die Möglichkeit auf Hazards zu reagieren und sie zu behandeln. Man kann sie beseitigen, abschwächen oder auch die Schwere eines resultierenden Unfalls reduzieren. Streng genommen ist das zwar kein Bestandteil der Analyse, es scheint jedoch ratsam Fehler direkt zu beseitigen wenn man sie findet.

Hat man alle Hazards behandelt, muss das verbleibende ‚Risiko, ermittelt werden. Hierfür bestimmt man:

- Die Auftrittswahrscheinlichkeit für jeden Hazard
- Für jeden Unfall der aus einem gegebenen Hazard resultieren kann die Wahrscheinlichkeit, dass, nach Eintreten des Hazards, der Unfall auch tatsächlich eintritt (Für diejenigen die mit Wahrscheinlichkeitstheorie vertraut sind: Die ‚bedingte Wahrscheinlichkeit eines Unfalls unter der Bedingung eines Hazards„.

Danach

- wird für jede Hazard/Unfall Kombination die Wahrscheinlichkeit des Hazard mit der bedingten Wahrscheinlichkeit des Unfalls unter der Bedingung eines Hazards kombiniert (wahrscheinlichkeitstheoretisch gesehen: multipliziert),

1 op.cit., Eintrag für ‚severity„

und durch die Schwere des Unfalls gewichtet (die Schwere hat normalerweise einen numerischen Wert, also bedeutet ‚gewichten' hier ‚multiplizieren,).

- werden anschließend diese einzelnen Resultate zu einem Gesamtergebnis kombiniert (bedeutet: ‚addiert,), welches man ‚Risiko, nennt.

Für die Wahrscheinlichkeitstheoretiker: Nimmt man an, dass die ‚Schwere, eine Zahl ist, und dass diese Zahl ein Maßstab für Verlust ist, dann habe ich hier gerade die Berechnung des *geschätzten Verlustwerts* beschrieben. Das ist kein Zufall. Weiterhin sollte man dazu sagen, dass diese Beschreibung des Prozesses nur dann korrekt ist, wenn ein gewisser Grad wahrscheinlichkeitstheoretischer Unabhängigkeit zwischen den Situationen deren Wahrscheinlichkeiten kombiniert werden existiert. Ist dies nicht der Fall, so müssen die Werte sachgemäß angepasst werden, um eine exakte Bewertung des zu erwartenden Schadens zu erhalten. Das behandele ich in Kapitel 5 TODO.

Nun wollen wir aber zu der Diskussion um Telefone auf Tankstellenhöfen zurückkehren.

## 1.2 Telefone auf Tankstellenhöfen: Kausale Analyse

Alle Diskussionsteilnehmer waren sich einig, dass auf Tankstellenhöfen entflammbare Gase (also ein entsprechendes Gas-Luft Gemisch) vorkommen können. Die Frage ist nur, ob und wie Mobiltelefone dieses entzünden könnten. (Brandschutzexperten sind sich normalerweise einig darin, dass man für ein Feuer drei Dinge benötigt: eine entflammbare Substanz, eine Sauerstoffversorgung und eine Zündquelle).

Niemand konnte jedoch genau sagen, warum die *Benutzung* von Mobiltelefonen an sich gefährlich sein sollte. Ja, es handelt sich um elektromagnetische (EM) Strahlenquellen, und die Benutzung von EM Strahlenquellen in möglicherweise explosionsgefährdeten Umgebungen ist normalerweise reglementiert. Aber welche Hazards gehen von der Benutzung von Mobiltelefonen aus?

John Ganter von Sandia Labs aus den USA wies darauf hin, dass es sich bei den Geschichten über Explosionen auf Tankstellen durch die Benutzung von Mobiltelefonen wohl um moderne Mythen handeln müsse:

> Die Geschichte von der Explosion ist 1999 im nationalen öffentlichen Radio gründlich aufgedeckt worden. Alle Versionen der Geschichte konn-

> ten auf eine frei erfundene Geschichte aus Südostasien zurückverfolgt werden. Hier wurde berichtet, dass die Ölkonzerne jedoch — warum auch immer — weiterhin an ihren Gefahrensticker-Kampagnen festhalten.
>
> `http://www.darwinawards.com/legends/legend1999-04.html`

> Der Exxon Pressesprecher Crawford Bunkley sagte, dass seine Firma nichts von irgendwelchen durch Mobiltelefone verursachten Feuern wüsste.
>
> Aber, ‚obwohl die Wahrscheinlichkeit einer Entflammung gering ist, halten wir diese Warnung trotzdem angesichts der Tatsche für angebracht, dass einige Mobiltelefonhersteller ihren Kunden raten ihr Telefon während des Tankvorganges auszuschalten.‘
>
> `http://www.austin360.com/entertainmenr/features/legend_cellphone.html`

Simon Brown von der UK Health and Safety Executive (HSE) vermutete, dass ein mögliches fallen lassen des Telefons einen Hazard darstellen würde. Warum? Weil sich die Batterie vom Telefon lösen und einen Funkenschlag erzeugen könnte. Diese Befürchtung wurde durch einem HSE Kollegen, an mich Simon verwiesen hatte, unterstützt.

Ein Mitglied der UK Safety Consultancy fragte ob es ‚veröffentlichte Daten über die elektromagnetische Feldstärke gäbe die notwendig wäre um verschiedene Gas-Luft Gemische zu entzünden‚. Simon Brown verwies ihn auf den britischen Standard (BS) 6656:1991 ‘Guide to the prevention of inadvertent ignition of flammable atmospheres by radio-frequency radiation’.

Natürlich ist es nicht nur der Funke allein der für eine Entflammung entscheidend ist, sondern auch die Energie die er beinhaltet. Niemand scheint sich Sorgen um Leute zu machen, die auf Tankstellenvorhöfen ihre Pullover ausziehen, obwohl, wenn der Pullover aus Kunstfaser besteht, spielend leicht dutzende oder gar hunderte Funken entstehen könnten.

Die benötigte Feldstärke um einen überspringenden Funken über einem Luftraum zu erzeugen (um den ‚avalance Effekt‚, wie Elektroingenieure und Physiker sagen, hervorzurufen) hängt im allgemeinen nur vom Luftdruck ab, und vom Abstand der Kontakte, falls dieser kleiner ist als etwa 1 cm.

Die Richtlinien des American Petroleum Institute für die Zündfähigkeit von Kraftstoff besagen (jedenfalls für Flugbenzin), dass für eine Entzündung 0,25 Millijoule (mJ) benötigt werden [67]. Laut einem Experten für die Entflammbarkeit von Flugbenzin, der von der NASA engagiert wurde um im Zusammenhang mit der TWA 800 über Funken zu berichten, liegt die ‚allgemein anerkannte, Kennzahl bei 0,2 mJ [12].

Daraufhin fragte ich: ‚Ob durch einen Funken oder nicht, wie soll man plötzlich 0,2 mJ aus einer Batterie bekommen, die mit 1000mAh bei 3V spezifiziert ist?‚

Die Antwort von John Dalton, einem Berater von Reflex Technology UK Ltd., war, dass die Kontakte kurzgeschlossen werden könnten. Seine Rechnung ging so: ‚[...] 2V x 10A x.00001s = 0.2 mJ. [Eine herkömmliche Mobiltelefon-] Batterie speichert über 10KJ [...]‚. Die Antwort, dass ein ‚zündfähiger Funke, theoretisch durch die Batterie eines Mobiltelefons erzeugt werde könnte, wurde (laut Simon Browns Kollegen) 1992 sowohl durch Untersuchungen der HSE, als auch durch meinen Kollegen Dr. Willi Schepper bestätigt. Willi Schepper ist Elektroingenieur und Physiker und beschäftigt sich mit elektromagnetischen Feldern in geschlossenen Räumen. Er erwähnte außerdem, dass das gleiche aber auch für alle anderen herkömmlichen Batterien gelte, wie sie zum Beispiel in Taschenlampen, Photoapparaten und Walkmans vorkommen. Mein Kollege Professor Harold Thimbleby, damals am University College London beschäftigt, fand es dennoch fraglich wie man es anstellen könnte, einen solchen Funken zu erzeugen. Also verbrachte er sein Wochenende freiwillig damit, mit Batterien und Propangas zu experimentieren (zum Glück weilt er noch unter uns :) ).

Nun, vielleicht lässt sich ein zündfähiger Funke durch eine simple Energiekalkulation nicht ausschließen, aber die Frage bleibt ob und wie die Kontakte der Batterie durch ein Fallenlassen des Mobiltelefons versehentlich so kurzgeschlossen werden könnten, dass ein solcher zündfähiger Funke entsteht.

Bei dem Design der Telefone die ich begutachtet habe fällt es mir physikalisch gesehen schwer zu verstehen, wie die Kontakte versehentlich kurzgeschlossen werden könnten. Bei zweien dieser Telefone, meinem Nokia 9110 Communicator und meinem Ericsson SH888 ist die Batterie extern, also ein Teil des Telefonkörpers. In zwei anderen, einem Siemens S35 und einem Motorola L7039 Timeport, ist die Batterie intern unter einer abnehmbaren Blende, welche zum Gehäuses gehört. In allen vier Telefonen sind die Batteriekontakte vier flache, etwa 2mm x 3mm große Metallplättchen, welche in das Batteriegehäuses versenkt sind. Bei dem 9110, dem SH888 und

dem S35 sind sie um etwa 1 mm in das Batteriegehäuse versenkt (beim S35 ist jeder Kontakt einzeln versenkt). Zusätzlich werden sie durch einen insgesamt mindestens 3 mm breiten, fließgepreßten Rand geschützt. Beim 9110 wird durch das an dieser Stelle ‚abgestufte, Batteriegehäuse sichergestellt, dass sich die Kontakte etwa einen halben Zentimeter innerhalb der ‚konvexen Schale, des Gehäuses befinden.

Die Kontakte der Batterie des L7039 werden nur durch die Ausmaße einer dicken Kunststoffummantelung geschützt, die die Batterie umgibt. Allerdings wird die Schale über der Batterie durch einen zweifach wirkenden Mechanismus geschützt: Zuerst muss ein in das Gehäuse eingelassener Knopf etwa 5 mm eingedrückt werden; gleichzeitig muss die Ummantelung um ca. 5 mm rechtwinklig zur Druckrichtung des Knopfes entlang des Gehäuses geschoben werden. Die gesamte Gehäuseschale wirkt robust. Selbst wenn das Telefon auf den Fußboden geworfen würde ist es schwer zu glauben, dass sie sich öffnen würde. (Simon Brown hat mir hingegen mitgeteilt, dass ihm sein LT7039 schon einmal heruntergefallen ist und die Batterie dabei abgesprungen ist.)

Weiterhin wird der Kontakt zwischen der Batterie und dem Telefon bei all diesen Telefonen über kleine Pins im inneren des Telefons hergestellt. Diese Pins sind gefedert; ich vermute, dass jegliche Bewegung der Pins (wie etwa beim Lösen der Batterie) gleichzeitig als Schalter fungiert, der das Telefon abschaltet bevor der Kontakt verloren geht – unter anderem um die Elektronik des Telefons vor Spannungsspitzen durch Funkenschlag zu schützen. Die Motivation der Telefonkonstrukteure die Zuverlässigkeit ihrer Produkte auf diese Art und Weise zu verbessern ist offensichtlich. Zuallererst möchten Sie natürlich, dass ihre Produkte den Ruf haben selbst bei mißbräuchlicher Benutzung zuverlässig zu sein. Weiterhin sind sie zum Beispiel in Europa gesetzlich verpflichtet, defekte Geräte bis zu einem Jahr nach dem Verkauf auszutauschen. Der Nachweis, dass ein Telefon durch unsachgemäße Handhabung zu Schaden gekommen ist kann sich selbst bei vorhandenem Verdacht schwierig gestalten.

Neben der Motivation die Zuverlässigkeit von PEDs (Personal Electronic Devices) wie Mobiltelefonen zu verbessern, gibt es weitere gute Gründe warum man Fehler durch Bogenentladungen in diesen Geräten verhindern sollte. Bogenentladungen erzeugen oft starke elektromagnetische Störungen. Es gibt viele Umgebungen, die empfindlich auf Elektromagnetismus (EM) reagieren. Einige von ihnen, wie zum Beispiel Verkehrsflugzeuge, besitzen sicherheitskritische elektronische Komponenten, welche durch EM Felder in der Kabine beeinflusst werden können. Durch Experimente

der britischen Zivilluftfahrtbehörde wurde vor kurzem nachgewiesen, dass ein innerhalb einer Flugzeugkabine strahlendes Mobiltelefon im Flugelektronikschacht eine Feldstärke von etwa 2 Volt/Meter bis 5 Volt/Meter erzeugen kann. Die angegebenen Interferenzimmunitätswerte von Flugelektronik genügen zwar nur dem Standard von vor 1984, werden jedoch durch diese Werte verletzt [4]. Dieser Standard kommt jedoch auch heute noch teilweise in neuen Flugzeugen zum Einsatz. Weiterhin liegen Luftfahrtbehörden einige Erzählungen von Flugzeugbesatzungen vor (z.B. über NASAs ASRS oder das britische CHIRPS System), die von Interferenzen während des Fluges berichten, die offensichtlich auf PEDs von Passagieren zurückzuführen sind. Bestätigt wurden diese zur Flugzeit durch Mills ‚Method of Differences, (die Flugbegleiter baten den Passagier das Gerät abzuschalten, und die Störung war verschwunden; dann baten sie um erneutes Einschalten, und die Störung war wieder da).

Aber zurück zu Telefonen und Tankstellenhöfen. Ja, auf Tankstellenvorhöfen kann es entzündliche Benzin-Luft Gemische an unvorhersehbaren Stellen geben. Ja, in den Batterien von Mobiltelefonen ist, ähnlich wie andere elektrische Geräte im Haushalt, genug ‚Saft, enthalten um eine Entladung von 0,2mJ oder mehr zu erzeugen. Ja, eine solche Entladung kann ein entflammbares Benzin-Luft Gemisch entzünden. Aber niemand konnte sagen, wie eine solche Entladung hervorgerufen werden könnte. Ein simpler Schaltmechanismus stellt sicher, dass die Elektronik isoliert wird sobald sich die Batterie anders als das Telefon bewegt. Und die Struktur der Kontaktstelle lässt sich nicht so leicht verformen. ‚Kurzschlüsse, zwischen den Batterieklemmen durch ungewolltes Zusammenkommen mit Stromleitern scheint durch die physikalische Konstruktion der Batterie effektiv verhindert worden zu sein, und damit auch die möglicherweise daraus resultierenden Funken.

Ich denke, das ist der Stand der Risiko-Analyse. Betrachten wir die Entzündung von brennbaren Dämpfen als den zu verhindernden Unfall, egal ob daraus Verletzungen resultieren oder nicht. Dann kann man hier zwei so genannte Hazards erkennen. Ein vermeintlicher ‚Hazard„ der anscheinend nicht zu einem Unfall führen kann, ist kein Hazard. Also sieht es so aus, als wäre die Verwendung oder auch das Fallenlassen eines Telefons schlicht und einfach kein Hazard.

Ende der Geschichte? Naja, nein, denn es ist eine Sache der öffentlichen Ordnung.

## 1.3 Telefone auf Vorhöfen: Safety Politik

Auf einigen Tankstellenvorhöfen ist die Benutzung von Telefonen explizit verboten. Simon Browns HSE Kollege vermutete, dass dies eine Richtline der Tankstellenbesitzer sei. Ein Leitfaden der HSE besagt, dass Angestellte ‚sicherstellen müssen, dass ... niemand tragbare elektrische/elektronische Geräte wie CB Funkgeräte oder tragbare Telefone benutzt"[69]. Der Nachdruck hinter einer solchen ‚Anweisung, kommt aus dem *UK Health and Safety at Work etc Act* von 1974, welcher unter anderem die Verantwortlichkeit eines Arbeitgebers gegenüber seinem Arbeitnehmer festlegt. Demnach muss dieser alle zumutbaren Schritte unternehmen, um die Sicherheit des Arbeitnehmers sicherzustellen und ihn so auszurüsten, dass er seine Aufgabe ohne Gefahr für sich oder andere ausführen kann (obiges Zitat mit anderen Worten).

Das Dokument sagt jedoch nichts darüber aus, wo der Angestellte mit der Unterbindung der Benutzung von Funksendern anzufangen hat. Ohne weitere Annahmen wäre es angebracht diese Regel auf dem kompletten Gelände als gültig zu betrachten. Entweder muss es so gemeint sein, oder es sind nur die Bereiche um die Benzinpumpen und Zapfsäulen gemeint. Zu diesem Schluss komme ich durch die folgenden Beobachtungen.

Simon Browns Kollege wies darauf hin, dass die Benutzung von Funksendern in Umgebungen, welche im Bezug auf einen explosiven Flächenbrand als gefährdet gelten, nur dann erlaubt ist, wenn jeder dieser Funksender einzeln für eine solche Benutzung zertifiziert worden ist. Als Beispiel: Das vom ‚Communications Advidory Panel, herausgegebene ‚UK Home Office Guidance HGN(F)15, rät, dass in einem Radius von 10 Metern um einen Bereich der als ‚potentiell explosionsgefährdet, gilt keine Funksendegeräte in Betrieb genommen werden sollten. Dieser Bereich wäre laut Brown genau der Bereich um die Benzinpumpen und Zapfsäulen. Daraus lässt sich die erste Interpretation ableiten. Das britische Institute of Petroleum Guidance for the construction and operation of petrol filling stations verlangt vor der Genehmigung einer Inbetriebnahme jeglicher Funksender, dass der Betreiber der Anlage diese zuerst begutachtet. Das leitet uns zur zweiten Interpretation. Weiterhin wurde ich darüber informiert, dass dies praktisch als eine Garantie des Ausrüstungslieferanten gilt, dass die Geräte für die Inbetriebnahme in einem eingeschränkten Bereich freigegeben sind.

Es gibt eine dritte, auf dem Gesetz beruhende Interpretation, nämlich die der Vor-

höfe von Tankstellen. Diese stammt aus dem ‚Highway code„ dem britischen Leitfaden für Verkehrsteilnehmer. Verstöße gegen diesen bilden die Basis für Verwarnungen durch die Polizei und Rechtsverfahren. Mark Coates von BAe Systems zitiert den Highway Code wie folgt:

> Tankstellen
> Auf den Vorhöfen von Tankstellen darf weder geraucht werden, noch dürfen Mobiltelefone benutzt werden, da beides eine große Brandgefahr mit sich bringt und zu einer Explosion führen kann.

Interessant ist, dass CB-Funkgeräte nicht erwähnt werden. Dies liegt vermutlich daran, dass es einfach nicht genügend davon gibt um die zusätzlichen Wörter zu rechtfertigen.

Bei dieser Gelegenheit sollte man mal all diese Hinweise über die Benutzung von Telefonen mit John Ganters Zitat des Exxon Pressesprechers Bunkley vergleichen. Dieses besagt, dass

> ‚einige Telefonhersteller [...] haben ihren Kunden aus Vorsicht geraten, beim Tanken ihre Telefone auszuschalten.,

Falls von der Funkübertragung eines Telefons tatsächlich ein Risiko ausgeht, dann besteht dieses auch dann, wenn das Telefon angeschaltet ist. Egal, ob damit ein Gespräch geführt wird oder nicht. Mobiltelefone die eingeschaltet sind, sich im so genannten ‚Standby-Modus, befinden, senden Statussignale um den Kontakt zu einer Basisstation zu halten. Wenn die übertragung tatsächlich ein Problem darstellen würde, sollten die Telefone in den besagten Gebieten komplett abgeschaltet werden.

Ich habe versucht herauszufinden, ob es zwischen dem Fallenlassen eines Telefons während der Benutzung und dem Fallenlassen eines eingeschalteten Telefons welches nicht benutzt wird einen für die Risikoabschätzung relevanten Unterschied gibt. Zumindest, ob sich die Wahrscheinlichkeit eines ‚zündfähigen Funkens, in beiden Fällen gleich ist, oder ob sie lieber als zwei verschiedene Hazards betrachtet werden sollten.

Ich vermute, dass in einem Telefon während der Benutzung größere Ströme fließen; also muss der Widerstand in der Elektronik im Telefon niedriger sein; und die Spannung in jeglichem Funken zwischen den Batteriekontakten und den elektrischen Komponenten des Telefons könnte höher sein. Aber die Möglichkeit, dass so ein Funke überhaupt entstehen kann, haben wir ja schon ausgeschlossen als wir uns die

Bauweise des Telefons angeschaut haben.

Wir müssen uns aber noch Gedanken um mögliche Funken machen, die durch Spannungsüberschlag zwischen den einzelnen Batteriekontakten entstehen, und nicht durch Spannungsüberschlag zwischen den Batteriekontakten und den Telefonkontakten. Nehmen wir an, sowohl der mechanische Ablauf als auch die Position in der ein Telefon fallengelassen wird sind relativ ähnlich, egal ob das Fallenlassen im Gespräch oder im Standby-Modus geschieht. Dann besteht der einzige für eine Risikoabschätzung relevante und erkennbare Unterschied also in den sich unterscheidenden Wahrscheinlichkeiten, mit denen das Telefon jeweils fallengelassen wird. Einmal, wenn man es während eines Telefonats relativ fest hält und auf der anderen Seite wenn es versehentlich herunterfällt während es im Standby-Modus ist weil man zum Beispiel in Handtasche oder Hosentasche nach Geld oder dem Autoschlüssel sucht. Naja, ich nehme an man bekommt keinen Preis wenn man errät, ob jemals jemand *diese* Wahrscheinlichkeiten ermittelt hat.

Es scheint, als würde niemand einen Grund kennen, warum die Situation in der ein Telefon auf einem Vorhof benutzt wird riskanter sein soll, als die eines zwar vorhandenen Telefons, welches sich aber im Standby-Modus befindet. Dies scheint auch von unbekannten Telefonherstellern in Bunkleys Zitat anerkannt zu sein. Sie fordern, dass das Telefon abgeschaltet wird. Das Verbot jeglicher Benutzung, nicht aber des Standby-Modus, wie vom HSE oder dem britischen ‚Highway Code, Leitfaden gefordert wird, genügt diesem Sachverhalt jedoch nicht. Außerdem sollte man nicht vergessen, dass niemand zu wissen scheint ob diese Situationen gemessen an den technischen Definitionen tatsächlich gefährlich sind.

Simon Browns Kollege bei der HSE schrieb mir, dass 1992 die Bauweise verschiedener Mobiltelefone untersucht, und mit den ‚anerkannten Standards für Ausrüstung vom Typ EX, (welche für nach meinem Verständnis die Standards für Funkausrüstungen mit Zulassung für explosionsgefährdete Bereiche sind) verglichen worden ist. Man kam zu dem Schluss, dass Mobiltelefone keinen der anerkannten Standards für eigensichere elektrische Ausrüstung für die Benutzung in ‚Zone 1, Gebieten erfüllen. Die dafür genannten Gründe waren: Zu hohe Batterieleistung, unzureichende Trennung von kritischen Komponenten, und inakzeptable Spannungsgrenzwerte bei Netzanschluss. Gemessen am britischen Standard (BS) 6941 für ‚Zone 2, Gebiete wurde das Spannungsniveau bei normaler Benutzung als sicher eingestuft, aber der durch die Plastikummantelung und Batteriekontakte gewährte Schutz konnte den

Vorgaben nicht gerecht werden.

Ich nehme an, seit dem hat es nicht zu vernachlässigende Fortschritte im Design von Telefonen gegeben. Der Experte hat mich jedoch darauf hingewiesen, dass die übereinstimmende Meinung seiner Kollegen auf diesem Gebiet sei, dass eine Untersuchung heutiger Geräte vermutlich zum gleichen Schluss kommen würde (Nur um das noch mal deutlich zu machen: Das ist eine Vermutung, kein Fakt).

Das erklärt, warum das Verbot jeglicher Verwendung existiert; es handelt sich um Funksender in einer stark feuergefährdeten Umgebung. Und die Verwendung solcher durch Angestellte wird durch HSE-Leitfäden gesetzlich geregelt. Außerdem sollen Tankstellenbedienstete dafür sorgen, dass niemand sein Telefon auf dem Firmengelände benutzt. Da stellt sich die Frage, warum dieses Verbot nicht klar und deutlich auf jedem Tankstellen-Vorhof in Großbritannien propagiert wird und sein halbgesetzlicher Zustand eindeutig ausgedrückt wird.

Firmen sind verpflichtet sich an diesen HSE Leitfaden halten. Ansonsten riskieren sie im Falle eines Unfalls eine Klage durch den HSE. Es ist jedoch nicht klar, ob und wie weit dieser Leitfaden durch gewöhnliche Bürger befolgt werden muss; er ist immerhin nicht an ein Gesetz gebunden.

Also scheint die Situation in Grossbritannien wie folgt auszusehen. Man darf ein Telefon auf Tankstellenvorhöfen benutzen, solange man dort nicht arbeitet. Wenn man dort allerdings ein Telefon benutzt muss man damit rechnen, dass ein Tankstellenbediensteter versuchen wird einen abzuhalten. Vermutlich wird er einem dabei mitteilen, dass das Telefon die erforderlichen Grenzwerte für Bereiche um Benzinpumpen und Zapfsäulen nicht einhält. Man darf ihn ungestraft ignorieren. Es könnte jedoch passieren, dass man, während man auf dem Tankstellenvorhof telefoniert, durch einen Polizisten aufgrund eines Verstoßes gegen den Highway Code verwarnt wird. Sollte man es darauf angelegt haben all diesen Personen auf die Nerven zu fallen, so könnte man sein Telefonat beenden und mithilfe seines Telefons, des Telefons seiner Frau und den Telefonen seiner Kinder an seinen Jonglierkünste arbeiten, während sich diese all diese Telefone im Standby-Modus befinden – wohl wissend, dass der Polizeibeamte nichts dagegen unternehmen kann, es dem Angestellten egal sein kann, und dass man sich keinerlei Risiko aussetzt.

Falls das nun alles einen etwas blödsinnigen Eindruck vermittelt möchte ich darauf hinweisen, dass Risikoabschätzungen wie sie durch das HSE durchgeführt werden zwar auf intuitiv plausiblen Prinzipien basieren, nicht jedoch notwendigerweise

auch auf technischen Risikoanalysen so wie sie am Anfang dieses Buches vorgestellt wurden. Betrachten wir also mal ein paar Methoden die üblicherweise zum Einsatz kommen, wenn Richtlinien unter fehlendem Fachwissen entworfen werden.

## 1.4 Einige Prinzipien

Hier ist die Analyse des ‚gesunden Menschenverstandes,. Telefone haben Batterien: Batterien enthalten genug ‚Saft, um einen Funken zu erzeugen, wenn sie auf einmal entladen werden. Dieser Funken enthält möglicherweise ausreichend Energie, um ein Benzin-Luft Gemisch zu entzünden. Durch unsachgemäße Handhabung könnte ein solcher Funken beim Lösen der Batterie und anschließenden Berührung der Kontakte mit einem überbrückenden Leiter erzeugt werden. Prinzip: Better be safe than sorry - Lieber auf Nummer Sicher gehen, als es nachher zu bereuen. (BBSFS) (Dieses Prinzip wird oft das ‚precautionary principle, genannt, was jedoch zu einem anderen Akronym führen würde welches von meinem kleinen Sohn für etwas völlig anderes benutzt wird.). Auf der Grundlage dieser Argumentation würde BBSTS anraten, dass Telefone auf Tankstellenvorhöfen auszuschalten sind.

Außerdem gibt es da noch den Angestellten-‚Leitfaden, für die Benutzung von Funksendern in Gebieten, die möglicherweise brandgefährdet sind. Also trifft ein weiteres bewährtes Vorgehensprinzip, das der ‚Prior Coverage, (PC, Vorsorge), zu. PC besagt: Telefone sind Funksender, Tankstellenvorhöfe sind erfasste und reglementierte Umgebungen: Diese Situationen werden durch existierende Leitfäden von Firmen durch die Empfehlung ‚don't use, (DU, Nicht benutzen) abgedeckt. Obwohl sie auf ähnlichen überlegungen basieren, wird durch PC ‚nicht benutzen„ durch BBSTS jedoch ‚abschalten, (switch off, SO) empfohlen. DU und SO sind logisch verwandt. Ein abgeschaltetes Telefon kann nicht benutzt werden. Dadurch wird DU notwendigerweise in jeglicher Situation befolgt, in der SO befolgt wird. Wir könnten auch sagen, dass SO mit DU direkt vergleichbar und mächtiger ist[1].

Hier ist ein weiteres Vorgehensprinzip, welches wir mal Like-Is-Like (LIL, gleiches mit gleichem) nennen. Dieses würde vorschlagen, der öffentlichkeit auf die gleiche Weise Ratschläge zu geben, wie sie auch Firmen ihren Angestellten (‚servant, im briti-

1 Das Zustandsprädikat, welches DU beschreibt, wird logischerweise durch das impliziert, welches SO ausdrückt.

schen Gesetz) und Subunternehmern (‚agent,) gegeben müssen. Für eine öffentliche Richtschnur zu Mobiltelefonen auf Tankstellenvorhöfen wird durch PC und LIL also das schwächere DU empfohlen, aber nicht das stärkere SO.

Die Argumentation, die bei BBSTS zu SO führt ist eine andere als die Argumentation die bei PC und LIL zu DU führt. BBSTS basiert auf der kausalen Kette, die zum Funken aus einer Batterie führt. PC basiert auf der Gefahr, die von Funkvorgängen ausgeht.

Was nun tatsächlich paßiert ist, dass man sich entschlossen hat der öffentlichkeit die Massnahme anzuraten die durch beide Verfahren impliziert wird – nämlich DU. Dieses Vorgehen könnte durch ein weiteres Prinzip namens ‚Multiple Justification, (MJ, mehrfache Bestätigung) gerechtfertigt werden: Wenn sich durch verschiedene, teilweise unabhängige überlegungen mehrere Ergebnisse ergeben, sollte das gewählt werden in dem die verschiedenen überlegungen miteinander übereinstimmen. In Unterhaltungen mit Vertretern der HSE wurde auch indirekt zur Verwendung von MJ geraten. Es scheint, als fühlt man sich wohler mit einer Empfehlung die durch mehrere, unabhängige überlegungen gerechtfertigt wird mit einer die nur aus eine einzelnen überlegung folgt.

Intuitiv scheinen all diese Prinzipien (BBSTS, PC, LIL und MJ) vernünftig zu sein. Wie es aber nun mal oft mit gesellschaftlichen Grundsätzen ist, ergeben sich Abweichungen von der Planung falls diese Grundsätze uneingeschränkt weitergegeben werden. Ein Beispiel: Eine verbreitete Kritik an der uneingeschränkten Anwendung von BBSTS ist, dass es zur gesellschaftlichen Lähmung, ‚Verletzung der Grundrechte, oder auch zu verschiedensten anderen in der Gesellschaft als unerwünscht angesehenen Phänomenen führen kann. Wird das LIL Prinzip wahllos angewandt, führt es zum ‚unternehmensgleichen Staat„ wie er angefangen mit John Kenneth Galbraith von so vielen Bürgern der westlichen Länder abgelehnt wird. In ähnlicher Weise ist PC ein sehr konservatives Prinzip, welches auch wieder von vielen, wenn auch nicht von allen, Bürgern der westlichen Welt abgelehnt wird. Daher muss über jegliche Anwendung dieser Prinzipien auch genauestens nachgedacht werden: Unüberlegte Anwendung dieser Prinzipien wird vom Gemeinwesen als nicht gerechtfertigt erachtet. Obwohl wir (und Organe wie die HSE) diese Aspekte ernst nehmen müssen, könnten wir die Einschränkung dieser Prinzipien vernünftigerweise Gesellschaftsphilosophen wie [2, 50, 63] überlassen. Dennoch halte ich es für legitim zu sagen, dass die Zuversicht der Politik in BBSTS, PC, LIL und MJ in sich widerspruchsfrei ist solange man die Einschränkung richtig trifft. Diese Kombination von Prinzipien ist es, die ich

während meiner Arbeit durch die Korrespondenz mit der HSE identifizieren konnte.

Nun möchte ich ein weiteres intuitiv vernünftiges Prinzip vorstellen: ‚Physical Causal Justification, (PCJ, technisch kausale Rechtfertigung). Im Prinzip besagt PCJ folgendes: Schlägt man eine Sicherheitsmaßnahme R für eine Situation S vor, dann tut man dies weil es Umstände gibt in denen eine Verletzung von R zu einem Unfall führt. Etwas ausführlicher kann man PCJ folgendermaßen beschreiben: Für jede Sicherheitsempfehlung R für bestimmte Gegebenheiten S muss es einen technischen Vorgang in bestimmten Gegebenheiten S geben, welcher in Situationen die mit S übereinstimmen zu einem Unfall führt, wenn alle Empfehlungen außer R befolgt worden sind und nur R verletzt wurde. PCJ sagt also aus, dass man Einschränkungen nicht aufgrund von Bedenken einführen soll, die physikalisch so nicht eintreffen können. Das ist ein Prinzip der realen Einschätzung kausaler Mechanismen.

PCJ ist der Grundsatz einer Verhaltensweise, die mit der technischen Risikoabschätzung verbunden ist. Egal was in der technischen Analyse als Hazard aufgeführt ist, wenn es keine kausale Kette gibt die von einer Situation S zu einem Unfall führt, dann ist die Wahrscheinlichkeit, dass ein Hazard zu einem Unfall führt, Null – denn aus der Situation S kann kein Unfall folgen. Ein sehr intuitives Prinzip welches ich ‚Don't Fret, (DF, Sorge dich nicht) nenne besagt, dass keine Maßnahmen ergriffen werden müssen wenn das Risiko Null ist. PCJ schildert die Situation, die als Ergebnis aus einer technischen Risikoabschätzung und der Anwendung von DF hervorgeht. Ich denke DF ist unbestritten.

Für safetykritische Artefakte wie Autos, Kraftwerke, Verkehrsflugzeuge, Flugleitsysteme oder auch die Chemieindustrie ist es notwendig, die technische Risikoanalyse so wie sie am Anfang dieses Buches vorgestellt werden durchzuführen. Viele dieser Risikoabschätzungen basieren auf epidemiologischen Studien (die zum Beispiel ermitteln könnten, welche gesundheitlichen Auswirkungen kleine Mengen von atmosphärischen Verunreinigungen wie Radon Gas in Häusern auf die Gesundheit haben) oder Zuverlässigkeitsstudien (die Wahrscheinlichkeit, dass ein bestimmter Systembestandteil technisch versagt) – es gibt jecoch auch viele die das nicht tun.

Grundsätze die auf der technischen Risikoanalyse (TRA) basieren sind nicht immer unumstritten. In der Erscheinung als RCBS (Risiko Kosten/Nutzen Analyse) ist sie

in starke Kritik geraten[1]. Diese Kritik ist hauptsächlich auf die Nutzung der eindimensionalen Metrik zur Beurteilung von Unfällen und ihrer Schwere gerichtet. Die Anwendung von RCBA setzt voraus, dass man z.B. einen direkten Vergleich zwischen der Verletzung eines Menschen und dem Schaden eines Artefaktes ziehen kann. Im Extremfall führt das dann schnell zu so beunruhigenden Phänomenen wie z.B. ‚dem finanziellen Wert eines Menschenlebens‚. Wie auch immer man zu solchen Themen steht, soll uns diese Diskussion im Moment nicht weiter beunruhigen, denn wir haben keinerlei Aussage darüber getroffen, wie die Schwere eines Unfalls zu klassifizieren ist. Bei unserem Streben nach technischen Risikoabschätzungen sind wir nicht gezwungen, einen Armbruch mit einem Beinbruch zu vergleichen oder irgendeine Verletzung mit den finanziellen Kosten einer erfolgreichen Behandlung – ganz zu schweigen von dem Vergleich mit einer Beule in einem Flugzeug. Aber im Sinne der RCBA sind diese alle direkt als ‚Kosten‚ vergleichbar. Eine auf RCBA basierende Richtlinie besagt: Minimiere die zu erwartenden Kosten (MEC, minimize expected cost). Es ist die Verwendung von MEC als Grundlage für Entscheidungen die oft zum Ziel für Kritik wird. Aber darum geht es uns hier einfach nicht. RCBA wird (wie andere Urteilsansätze auch) zwar durch die TRA unterstützt, geht jedoch über das was die TRA fordert hinaus. MEC ist nur dann als Grundsatz kohärent, wenn diese weiteren durch RCBA geforderten Schritte gegangen werden. Wir werden uns an dieser Stelle aber nicht weiter mit diesen Schritten befassen, die Diskussion um MEC steht also weiter aus.

Ein wichtiges Beispiel für die Anwendung von TRA (abgesehen von der RCBA) ist die Untersuchung von Unfällen mit Verkehrsflugzeugen, zu der sich die Unterzeichner der Chicago Convention 1948, die die International Civil Aviation Organisation (ICAO) bilden, verpflichtet haben. Der Sinn solcher Untersuchungen liegt in der Identifikation der tatsächlichen technischen Risiken durch die sorgfältige und kausale Analyse von Unfällen die sich ereignet haben. Die dabei identifizierten Risiken müssen nicht zwangsläufig mit dem eigentlichen Unfall an sich in kausaler Verbindung stehen – es ist durchaus vorgekommen, dass bei der Untersuchungen eines Unfalls Risikophänomene identifiziert wurden die für diesen Unfall jedoch nicht kausal waren. Die überwiegende Mehrheit an Empfehlungen basiert jedoch auf Faktoren die für Unfälle kausal waren. Die technische Risikoanalyse wie ich sie hier umrissen habe ist

1 Eine Diskussion zu dem Thema kann z.B. in [62, 63] oder in der Zeitschrift ‚Risk Analysis‚ gefunden werden

zu kausalen Untersuchungen von Unfällen komplementär. Erstere sind dazu bestimmt alle Möglichkeiten zu identifizieren nach denen ein Unfall passieren könnte. Durch ihren kontrafaktischen Charakter wird es dementsprechend schwerer dieses Ziel zu erreichen als es bei einer Unfallanalyse der Fall ist, wo es ja unter anderem darum geht den genauen Unfallhergang wie er tatsächlich passiert ist aufzudecken.

Stellen wir nun die Behauptung auf, dass eine (korrekt durchgeführte) technische Risikoanalyse in jedem Fall zweckmäßig ist: Wird eine solche durchgeführt, liefert sie unbestreitbar relevante Informationen für eine Risikoabschätzung. Nennen wir diese Behauptung TRA Validity (TRAV, TRA Gültigkeit). Ich bin der Auffassung, dass TRAV unter den meisten Experten unbestritten ist. Ich kenne kein Beispiel in der Literatur, dass auf schlüssige Weise Einwände gegen TRAV hervorbringt. Mit Hilfe von TRAV können wir nun den Beweis, der PCJ durch eine TRA zusammen mit DF stützt, wie folgt formulieren: Aus TRAV + DF folgt PCJ. Die Unanfechtbarkeit sollte durch diese Schlußfolgerung erhalten bleiben, jedenfalls nach allen Kriterien der Vernunft. Also folgt daraus, dass auch PCJ unanfechtbar ist.

Man sollte sich nicht dazu verleiten lassen diese Beweiskette so zu interpretieren, dass PCJ nur dann unanfechtbar ist wenn eine TRA tatsächlich durchgeführt worden ist. Das Prinzip TRAV ist allgemeingültig. Seine Aussage beruht nicht darauf, dass tatsächlich eine TRA durchgeführt wurde sondern einfach auf der Definition eines Risikos. PCJ ist uneingeschränkt unanfechtbar.

Von den Prinzipien über die wir hier gesprochen haben, ist PCJ das am besten begründete. Durch seine Beziehung zur technischen Risikoanalyse und die uneingeschränkte Unanfechtbarkeit ist PCJ wohl auch das wichtigste der oben genannten Sicherheitsprinzipien. PCJ kann jedoch nicht durch die Verknüpfung der Prinzipien BBSTS, PC, LIL und MJ sichergestellt werden. Die Empfehlung der HSE bezüglich Mobiltelefonen auf Tankstellenvorhöfen ist da ein gutes Gegenbeispiel. Wie wir gesehen haben, ist diese Empfehlung sowohl offen als auch indirekt durch BBSTS, PC, LIL und MJ gerechtfertigt. Aber ich habe darauf hingewiesen, dass sie, soweit wir das beurteilen können, PCJ verletzt.

Dies befördert die Entscheidungsträger wie das HSE in eine schwierige Position. Wenn keines der Prinzipien BBSTS, PC, LIL und MJ die Erfüllung von PCJ sicherstellen kann, diese aber nichtsdestotrotz sichergestellt werden muss da es unanfechtbar ist, dann gibt es keinen kürzeren Weg um PCJ sicherzustellen. Wenigstens eine TRA auf irgendeinem Level muss durchgeführt werden. Außerdem muss man sich

nach der Rechtfertigung von jedem der Prinzipien BBSTS, PC, LIL und MJ fragen. Diese Prinzipien schaffen es weder alleine noch alle zusammen PCJ zuverlässig zu ersetzen. Andernfalls wären sie ja in der Lage PCJ bestätigen. Wenn sie jedoch keinen verlässlichen Ersatz für TRA darstellen, wie sollte man ihren Einsatz dann begründen?

Ich glaube, dass BBSTS, PC, LIL und MJ eine TRA in genau den Fällen ersetzen können, wo man das Gefühl hat, dass das identifizierte Risiko die Kosten für eine vollständige PCJ nicht rechtfertigen würde. Aber wie der Fall mit den Telefonen auf den Tankstellenvorhöfen gezeigt hat, reichen diese Prinzipien nicht als Ersatz für eine TRA aus. PCJ muss, wenigstens in seiner schwächsten Form einen kausalen Pfad zu einem Unfall aufzudecken, unabhängig von diesen vier anderen Prinzipien abgesichert werden.

Dieses Buch beschäftigt sich mit der Ermittlung und Analyse kausaler Pfade. Zum einen mit potentiellen kausalen Pfaden, die in noch der Entwicklung steckende Systeme möglicherweise einmal zu Fehlfunktionen oder unsicherem Betrieb führen können, als auch mit tatsächlichen kausalen Pfaden wie sie vor Fehlfunktionen und Unfällen bereits aufgetreten sind. Die Analyse der Kausalität erlaubt die Zuhilfenahme einer genauen Wissenschaft, was bei den anderen Prinzipien nicht der Fall ist. Jedenfalls nicht offensichtlich.

Zuerst werde ich einige der sozialen und psychologischen Hintergründe des technischen Risikos unter die Lupe nehmen.

Ôªø