Funktionale Sicherheit - Gesamtbetrachtung

Ingo Rolle

Zuverlässigkeit, Funktionale Sicherheit und Qualität
von (elektro-)technischen Systemen

Hochschule Darmstadt
University of Applied Sciences
Fachbereich EIT

30. Juni 2017

Inhaltsverzeichnis

Einleitung **I**

Lernziele **III**

1. Einige Fälle von Versagen eingebetteter Systeme **5**

1.1 Überlauf eines Lagertanks ... 5

1.2 Verlust des Mars-Polar-Landers ... 9

1.3 Versagen des Blow-Out-Preventers der Deep-Water-Horizon-Bohrplattform ... 10

1.4 Beschädigung iranischer Urananreicherungsanlagen durch die Schadsoftware „Stuxnet“ ... 12

2. Der Sicherheitsbegriff nach ISO/IEC Guide 51 und Vorstellungen, Sicherheit zu erreichen **17**

2.1 Der ISO/IEC Guide 51 ... 17

2.2 Anwendungsbeispiel ... 20

2.3 Umsetzung in den einzelnen Branchen ... 21

2.4 Reflexion ... 22

3. Die Vorstellungen zum Erreichen von Sicherheit in elektrotechnischen Sicherheitsnormen **25**

3.1 Modelle ... 25

3.2 Grenzen der Vorstellungen der elektrotechnischen Sicherheitsnormen ... 28

3.3 Merkmale elektrotechnischer Sicherheitsnormen ... 30

3.4 Reflexion ... 32

4. Die Vorstellungen zum Erreichen von funktionaler Sicherheit nach DIN EN 61508 (VDE 0803) **33**

4.1 Definition der funktionalen Sicherheit ... 33

4.2 Modelle der funktionalen Sicherheit ... 34

4.2.1 Risikoreduktionsmodell ... 35

4.2.2 Ausfallmodell ... 36

4.2.3 Modell 4 ... 37

4.2.4 Grenzen der Vorstellung zum Erreichen funktionaler Sicherheit ... 39

4.3 Umsetzung in den Normen ... 41

4.4 Übernahme der IEC 61508 in die Fachgebiete ... 44

4.5 Prozessbezogene Norm versus konkrete Produktanforderungen 48
4.6 Gestufte Anforderungen 49
4.7 Reflexion 51

5. Sicherheitsfunktionen 53

5.1 Beispiele für Sicherheitsfunktionen 53
5.1.1 Tanküberlaufschutz 53
5.1.2 Mars Polar Lander 53
5.1.3 Blow Out Preventer 54
5.1.4 Papierschneidemaschine 54
5.1.5 Fahrerloses Transportfahrzeug 56
5.1.6 Notstromversorgung 56
5.1.7 Fehlerstromschutzschalter RCD Typ B 57
5.3 Spezifikation von Sicherheitsfunktionen 70
5.4 Reflexion 71

6. Betriebsmittelkennzeichnungen und Aufgabendarstellungen in einem R&I-Fließbild 73

6.1 PCE-Aufgaben, PLT-Stellen und Tag-Number 73
6.2 Das Verwechslungsproblem 75
6.3 Reflexion 75

7. Lösungshinweise zu den Aufgaben 79

8. Literaturverzeichnis 83

Einleitung

In unsere technische Umgebung halten immer mehr mikrorechnerbasierte Systeme Einzug. Bei neuen Anwendungen steht zunächst der erwartete Nutzen im Vordergrund der Diskussionen. Sind die intelligenten Systeme oder „smarten Helfer“ jedoch erst einmal vorhanden, ist es naheliegend, ihnen auch Schutzaufgaben zu übertragen oder sie Sicherheitsfunktionen ausführen zu lassen. Sie wachen daher heute über den richtigen Druck im Reaktionskessel von Anlagen der chemischen Industrie, unterbinden Überläufe von gefährlichen Flüssigkeiten, verhindern Unfälle im Umgang mit Maschinen, steuern Roboter und kontrollieren die Kräfte im Bremssystem in unserem Automobil. Wir sprechen von eingebetteten Systemen, wobei die erwähnten Sicherheitsfunktionen eine Teilmenge ihrer Aufgaben bilden.

Die Menschen möchten auf diese Helfer in ihrer Umgebung vertrauen können und erwarten hierfür eine entsprechend befähigte Technik. Funktionale Sicherheit und Informationssicherheit sind die Werkzeuge des Automatisierungsingenieurs, um dafür zu sorgen, dass die Sicherheitsfunktionen richtig ausgeführt werden und unerlaubte Handlungen nicht die Hilfe der elektronischen Systeme in eine böse Überraschung verkehren können.

Funktionale Sicherheit bedeutet hierbei die Fähigkeit, die festgelegten Sicherheitsfunktionen zuverlässig und spezifikationsgemäß auszuführen. Die Auslegungsgrundsätze für Systeme, die diese Fähigkeit aufweisen, sind Gegenstand der siebenteiligen Reihe der Internationalen Sicherheitsgrundnormen IEC 61508, sie wurde in das deutsche Normenwerk als Reihe DIN EN 61508 (VDE 0803) übernommen, siehe auch [1] bis [7]. Systeme, die Sicherheitsfunktionen ausführen, werden in der Norm sicherheitsbezogene Systeme genannt, üblich sind auch die Benennungen "sicherheitsgerichtete Systeme" oder "sichere Systeme".

Das Ziel der Informationssicherheit (diese Benennung wird als synonym zu „Cyber-Security“ angesehen) ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, die ein System verarbeitet, sicherzustellen. (Je nach Betrachtungsweise können weitere Ziele hinzutreten). Diese Informationen können zur Ausführung von Sicherheitsfunktionen dienen oder auch nicht. Ein möglicher Angreifer könnte beispielsweise versuchen, die Ausführung einer Sicherheitsfunktion zu stören und damit Gefahren herbeizuführen oder aber er kann unbemerkt vertrauliche Informationen gewinnen, ohne dass ein Sicherheitsproblem auftritt. Aus diesem Grunde ist es nicht vorteilhaft, die Informationssicherheit als Spezialdisziplin der funktionalen Sicherheit aufzufassen. Die Auslegungsgrundsätze für eingebettete Systeme, die Eigenschaften der Informationssicherheit aufweisen sollen, sind indes noch nicht fest gefügt, es gibt hierzu noch keinen "Stand der Technik". Dieser wird gerade erst im Rahmen der internationalen Normung (IEC 62443, vorgesehen als VDE 0802) erarbeitet. Im Modul

5.3 wird eine Vorausschau gegeben und diese mit den Grundsätzen der funktionalen Sicherheit verglichen werden.

Diejenigen Anwendungsgebiete, in denen eingebettete Systeme eingesetzt werden, haben oft ihre eigene Vorgehensweise zur Erreichung von Sicherheit, eine "Sicherheitsphilosophie", die mit den Betrachtungsweisen der funktionalen Sicherheit und der Informationssicherheit nicht unbedingt übereinstimmt. Insbesondere die Vorgehensweise der klassischen Elektrotechnik zur Erreichung von Sicherheit ist hier zu nennen. Mindestens Verständnisprobleme sind daher die Folge. Sie behindern in der Praxis die angemessene Behandlung von funktionaler und Informationssicherheit in neuen Anwendungen und damit letztlich den Einsatz eingebetteter Systeme in diesen. In diesem Modul werden daher die gemeinsamen Grundlagen zur Erreichung von Sicherheit vorgestellt, die unterschiedlichen Vorgehensweisen in den angesprochenen Gebiete verglichen (die Informationssicherheit wird im Modul 5.3 hinzugenommen) und auf die Anwendungsgrenzen aufmerksam machen, denn die allein gültige "Sicherheitsphilosophie" gibt es nicht.

Damit wird die Voraussetzung für den Entwurf, die Realisierung und den Betrieb sicherer Systeme als interdisziplinäre Arbeit geschaffen. "Einbettung“ bedeutet daher nicht nur die Verbringung des Mikrorechner-Systems in eine besondere technische Umgebung, sondern auch in eine besondere menschliche, mit eigener Nomenklatur und Vorstellungswelt.

Lernziele

Die Einführung des Sicherheitsbegriffs nach ISO/IEC Guide 51 als Grundlage für fachübergreifende Betrachtungen

Kennenlernen des Gefährdungs- und Risikoreduktionsmodels, das vielen Normen der elektrischen Sicherheit zugrunde liegt. (Beispiel IEC 62368, in Deutschland übernommen als DIN EN 62368-1 (VDE 0868-1))

Kennenlernen des Risikoreduktionsmodells der IEC 61508 sowie deren Ausfallmodelle.

Klassifizierung von Sicherheitsfunktionen, ihren Spezifikationen und den ausführenden Systemen

Bedeutung von Kennzeichnungssystemen am Beispiel von Fließbildern der Verfahrenstechnik und Übungen zur Einführung in die Risikoanalyse und -bewertung.

Dadurch, dass der Studierende die Grundlagen der funktionalen Sicherheit kennenlernt, kann er diese auch in neuen Applikationen und neuen technischen Gebieten anwenden.

die Schreibweise „IEC 61508“ schließt in diesem Lehrbrief die deutsche Fassung DIN EN 61508 (VDE 0803) mit ein und umgekehrt. Verweise auf die IEC 61508 und die DIN EN 61508 (VDE 0803) sind als gleichwertig zu betrachten). Entsprechendes gilt für die noch zu erwähnenden weiteren internationalen Normen.

1. Einige Fälle von Versagen eingebetteter Systeme

Die beste Erkenntnisquelle zum Thema Sicherheit für den praktisch tätigen Ingenieur/Ingenieurin sind Fälle von Versagen technischer Systeme, also Unfälle, die sich ereignet haben, sowie gefährliche Vorfälle. Selten werden diese jedoch näher untersucht und das Ergebnis öffentlich zugänglich gemacht. Einige solcher Veröffentlichungen stehen uns dennoch zur Verfügung. Sie geben uns die Möglichkeit, aus vorgekommenen Fehlern zu lernen in dem Bewusstsein, dass auch wir nur Menschen mit Schwächen sind, die Fehler machen. Auch im Zeitalter hochwertiger Sicherheitstechnik sollten wir nicht vergessen, dass jede Technik nur so gut und so sicher ist, wie die Menschen, die sie bauen, betreiben und in Stand halten. Das gilt umso stärker, je mehr Funktionen automatisiert sind.

Die Beispiele werden von Ihnen verlangen, sich in die verschiedensten technischen Anwendungsgebiete hineinzuversetzen, was jedoch dem interdisziplinären Charakter dieses Studienganges geschuldet ist.

1.1 Überlauf eines Lagertanks

Unter dieser Überschrift sei ein persönliches Erlebnis des Autors wiedergegeben. Das Unternehmen der Mischfutterindustrie, in dem sich der Fall ereignet hat, ist inzwischen von der Bildfläche verschwunden, ebenso wie das einst stolze Werk, das wir damals in einem Hafen Norddeutschlands neu errichtet hatten. Mischfutter für landwirtschaftliche Nutztiere ist – wie der Name bereits nahelegt – eine Mischung der verschiedensten Inhaltsstoffe, darunter auch flüssige. Ein besonders wichtiger davon ist Melasse, ein Nebenprodukt der Zuckerindustrie, das jeweils zur jährlichen Zuckerrübenkampagne in großen Mengen anfällt und dann im Laufe des Jahres über die Mägen der Kühe und die verschiedensten Milchprodukten doch noch der menschlichen Ernährung zugeführt wird. Melasse ist ein brauner Sirup, in ähnlicher Form auch als Brotaufstrich verwendet, der an benetzten Oberflächen klebrigen Schlamm und kristalline Anbackungen hinterlässt. Aus diesem Grunde hatten wir einen gehörigen Respekt vor dieser Komponente, auch wenn sie nicht als wassergefährdend eingestuft ist. Einen Überlauf des neuen, direkt an einer Kaimauer errichteten Lagertanks wollten wir deshalb unter allen Umständen verhindern. Melasse muss im Winter beheizt werden, damit sie pumpbar bleibt, so dass der Tank mit einer Steinwolleschicht umgeben und schließlich mit Blechplatten eingehaust wurde, siehe Abb. 1.1. Das Volllaufen dieser Steinwolleschicht betrachteten wir als besonders zu vermeidende Störung, ebenso wie eine Verschmutzung der umliegenden Maschinen und Anlagenteile.

Befüllt wurde der Tank aus LKWs, die die Melasse mit eigener Pumpe über einen nicht mitgezeichneten Stutzen in den Tank hineinpumpten. Über eine ebenfalls nicht mitgezeichnete Rohrverbindung wurde der Tankinhalt abgezogen und mit Hilfe einer

Pumpe in ein höheres Stockwerk gepumpt und dort verarbeitet. Eine betriebliche Füllstandsmessung sollte dem Personal anzeigen, wieweit der Tank noch gefüllt war und wann ein neuer LKW zu bestellen war.

Der Begriff „funktionale Sicherheit“ war noch nicht zu uns vorgedrungen, aber als Elektrotechniker wussten wir, dass man sich gegen den ersten und – wenn man besonders sicher gehen wollte – auch gegen den zweiten Fehler sichern sollte. Für den Fall, dass die betriebliche Füllstandsmessung nicht funktionieren sollte, sahen wir deshalb zwei Schutzmaßnahmen vor:

- einen Füllstandsgrenzschalter, links oben im Bild, der an eine SPS angeschlossen war. Erreichte der Melassespiegel diesen Schalter, sollte die SPS einen Alarm in der Schaltwarte des Werkes und einen weiteren akustischen Alarm direkt am Tank auslösen. Letzterer sollte dann den LKW-Fahrer veranlassen, die Pumpe auf seinem Fahrzeug abzuschalten
- ein schwanenhalsähnliches Rohr, rechts oben gezeichnet. Wäre in den bereits vollen Tank immer weiter Melasse hineingepumpt worden, wäre diese hier ausgetreten und dem LKW-Fahrer sozusagen direkt vor die Füße gelaufen, um ihn damit dazu zu bringen, seine Pumpe abzustellen.

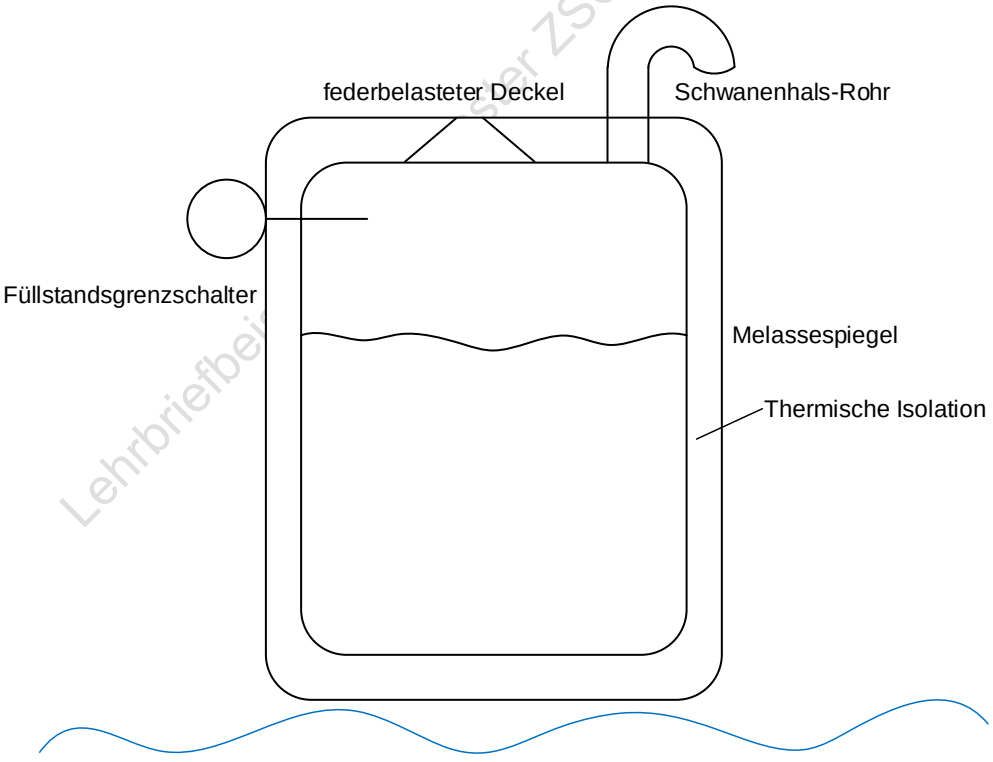

Abb. 1.1: Tank mit Schutzeinrichtungen

Damit, so meinten wir, hätten wir nach dem Stand der Technik sehr viel getan, um einen derartigen Störfall abzusichern. Und so nahm das Schicksal seinen Lauf.

Die SPS, an die der Füllstandsgrenzschalter angeschlossen war, steuerte den gesamten, recht komplexen Produktionsprozess im angrenzenden Gebäude. Die entsprechenden Programmteile wurden gründlich getestet. Das Programm zum Tanküberlaufschutz wurde jedoch als einfach eingestuft, war zur Abnahme im Herstellerwerk noch nicht fertig und wurde infolgedessen auch nicht mitgeprüft.

Alle Aggregate wurden an den Tank angeschlossen und die Verbindung zur SPS hergestellt. Ein Inbetriebnahmeteam prüfte anschließend den Füllstandsgrenzschalter. Eine Leiter wurde an den Tank angelegt, jemand stieg hinauf und betätigte einen Prüfschalter am Füllstandsgrenzschalter. Der Alarm wurde ausgelöst und die Prüfung damit erfolgreich abgeschlossen. Angemerkt sei, dass es Januar war und schlechtes Wetter an jenem Tag.

Die betriebliche Füllstandsmessung beruhte auf der Erfassung des hydrostatischen Drucks. Das Justieren dieser Messeinrichtung setzte einen leeren Tank voraus, Dies fand nicht zum geplanten Zeitpunkt statt, weil nicht genügend Inbetriebnahmeingenieure auf der Baustelle waren. Deshalb wurde der Tank befüllt, ohne auf die Inbetriebnahme zu warten. Folglich funktionierte diese Messstelle nicht, auch danach wurde der Tank nicht mehr vollständig entleert.

Der Rohwarendisponent hatte zwar die Füllstandsmessung nicht zur Verfügung, verfolgte aber die innerbetriebliche Bestandsfortschreibung. Einige Monate lang gelang es ihm, einen neuen LKW stets dann zu bestellen, wenn noch genügend Platz im Tank war. Doch eines Tages kam, was unvermeidlich war: Er bestellte zu früh. Der nichtsahnende LKW-Fahrer ließ die Pumpe seines Fahrzeuges laufen und bemerkte plötzlich, wie die Melasse am Fuß des Tanks aus dessen Verkleidung herausgedrückt wurde. Keine einzige der Schutzeinrichtungen hatte funktioniert. Die Verkleidung musste entfernt werden, die Isolation war vollgesogen und ein Fall für die Müllentsorgung. Sogleich wurde offenbar, weshalb die Alarmierung durch den Schwanenhals nicht funktioniert hatte. Der Tank hatte einen federbelasteten Deckel, um im Falle einer Explosion oder eines Brandes für Druckentlastung zu sorgen. Der hydrostatische Druck der ansteigenden Melasse reichte aus, um den Deckel ein wenig anzuheben und ihr den Weg in die Steinwolle-Isolationsschicht freizumachen. Melasse ist übrigens nicht brennbar und kann auch nicht explodieren. Für dieses Medium war es schlicht der falsche Tank.

Doch weshalb gab die SPS keinen Alarm?

Von dem Füllstandsgrenzschalter, der den Hochalarm auslösen sollte führte ein binäres 24 V Signal zum Eingang des SPS und in deren Programm zu einer entsprechen-

den boolschen Variablen. Sie wurde einem Programmodul übergeben, das kurzzeitige Impulse unterdrücken und eine längere Bedeckung des Sensors mit Flüssigkeit dauerhaft als boolsche Variable abspeichern sollte („Entprellen“). Dieses Modul funktionierte nach jedem Rücksetzen der SPS einmal und wartete anschließend auf das Rücksetzen einer Hilfsvariablen aus dem umgebenden Applikationsprogramm. Dummerweise war dies nirgends dokumentiert und der Anwendungsprogrammierer wusste es nicht. Das Modul funktionierte beim Test das erste und das letzte Mal, denn die SPS steuerte auch die Produktion und wurde im normalen Betrieb nicht mehr zurückgesetzt. Beim Test wurde zwar der akustische Alarm und die Anzeige quittiert, nicht jedoch der entscheidende Hilfsmerker zurückgesetzt, weil dies im Programm nicht vorgesehen war. Bei einer Wiederholung des Tests wäre dies aufgefallen, die unterließ das Inbetriebnahmeteam jedoch, weil das Betätigen des Testschalters auf einer Leiter bei schlechtem Wetter wenig einladend war.

Damit konnten wir unsere Ursachenforschung abschließen:

- ein Kollege hatte einen falschen Tank bestellt
- ein Programmodul war nicht ausreichend dokumentiert

Außerdem mussten wir feststellen, dass unsere Strategie, mehrere Schutzmaßnahmen gestaffelt aufzubauen, keinen Erfolg gehabt hatte.

Aus heutiger Sicht dürfen wir folgende organisatorische Ursachen hinzufügen:

- in diesem Projekt gab es zu wenig klare Strukturen, es wurde zu viel auf Zuruf erledigt.
- Es gab auch niemanden, der diese Schutzeinrichtungen beurteilen und freigeben sollte
- Die Prüfungen (Verifikation und Validierung) waren nicht gründlich genug, sie erfolgten nicht schrittweise mit der Errichtung des Systems sondern nur einmal ganz am Schluss
- Der Tank wurde vor der Isolierung nicht begutachtet
- Es ist auffällig, dass beim Aufbau des Tanks niemand den überflüssigen, federbelasteten Deckel bemerkte. Das Gewerk wurde nicht ausreichend von jemandem beaufsichtigt, der die Funktionsweise der gesamten Anlage kannte.

Die Natur der vorgesehenen Schutzeinrichtungen brachte jedoch auch einige prinzipielle Schwierigkeiten mit sich:

- Andere risikomindernde Maßnahmen – so bezeichnet die IEC 61508 nichtelektrische Systeme wie die Schwanenhalskonstruktion – sind oft schwierig zu prüfen. Denn man wird in der Praxis keinen Tanküberlauf absichtlich herbeiführen wollen.

- Schutzmaßnahmen, die nur selten benötigt werden, sind laut IEC 61508 „Sicherheitsfunktionen, die in der Betriebsart mit niedriger Anforderungsrate betrieben werden“. Zwischen zwei wiederkehrenden Prüfungen können sie unerkannt ausfallen, so dass sie dann im Anforderungsfall nicht zur Verfügung stehen.

1.2 Verlust des Mars-Polar-Landers

Das Absetzen einer Sonde auf der Marsoberfläche wird zwar üblicherweise nicht als Ausführung einer Sicherheitsfunktion angesehen, jedoch lagen auch hier hohe Erwartungen an die Zuverlässigkeit der ausführenden Technik vor, so dass ein Vergleich erlaubt sei. Den Fall des Mars Polar Landers hat Nancy Leveson in ihrem bekannten Aufsatz über Software-Versagen in Raumfahrzeugen sehr gut dokumentiert [8].

Die Rakete mit dem Mars Polar Lander als Nutzlast wurde im Januar 1999 mit dem Ziel gestartet, eine Sonde am Südpol des Mars abzusetzen, um dort wissenschaftliche Erkundungen durchzuführen. Am 3. Dezember jenen Jahres war es soweit: die Landung wurde eingeleitet. In ihrem Verlauf wurden die Bremsraketen für die Landung gezündet, die Landefüße auseinandergefaltet und in ihrer Endposition eingerastet. Dies geschah ohne Kommunikation mit der Erde. Die Kommunikation mit der Sonde konnte jedoch nicht wie vorgesehen wieder aufgenommen werden, sie war offensichtlich verloren gegangen.

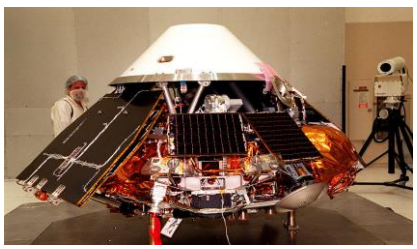

Abb. 1.2: Mars Polar Lander (Bildquelle: Wikepedia)

Die später durchgeführte Untersuchung ergab als wahrscheinlichen Ablauf folgendes: Das Landungsprogramm sah vor, dass bei Berührung der Marsoberfläche die Bremsraketen abgestellt werden sollten. Die Berührung sollte mit Hilfe von Hall-Sonden in den Landefüßen erkannt werden. Beim Auseinanderfalten der Landefüße während des Landeanflugs gaben diese Sonden ebenfalls einen kurzen Impuls ab. Zur richtigen Funktion hätte die Software, die den Landevorgang steuerte, diese Impulse nicht auswerten dürfen, sondern hätte sie übergehen müssen. Die Untersuchung ergab, dass die Software diese Eigenschaft nicht aufwies, so dass die Bremsraketen wahrscheinlich bereits beim Auseinanderfalten der Landefüße abgeschaltet wurden, die Sonde daher nicht weiter abgebremst wurde, auf der Marsoberfläche aufschlug und dabei zerstört wurde. Nancy Leveson nennt in ihrem Aufsatz folgende Faktoren, die zu diesem unglücklichen Ablauf beitrugen:

- die Spezifikation für die Steuerungssoftware der Landung erwähnte die Signale durch das Auseinanderfalten nicht und forderte auch nicht, diese zu verwerfen. Die Software arbeitete also im Hinblick auf ihre Spezifikation richtig. Es handelte sich um einen Spezifikationsfehler. (Im Gegensatz zu dem Beispiel mit dem Tanküberlauf. Hier waren die Funktionen zwar korrekt spezifiziert, es mangelte jedoch an der Ausführung)
- die Sensoren und ihr Verhalten wurden zwar geprüft, aber die Programmierer der Steuerungssoftware kannten nicht die Ergebnisse dieser Untersuchung.
- die Software wurde nur in Modulen getestet. Es gab keinen Test mit dem verbauten eingebetteten System, seiner Software und möglichst einem großen Teil der zugehörigen Aktorik und Sensorik
- bei den Tests der Software-Module war niemand anwesend, der das Verhalten des Gesamtsystems überblickte. Auch hier waren also, wie auch beim erwähnten Tanküberlaufschutz, die Tests nicht gründlich genug. Dazu ist jedoch anzumerken, dass Tests oft schwierig zu organisieren sind, da die vorgesehene endgültige Umgebung nicht zur Verfügung steht oder das zu beherrschende Ereignis nicht herbeigeführt oder hinreichend simuliert werden kann.

1.3 Versagen des Blow-Out-Preventers der Deep-Water-Horizon-Bohrplattform

Der Ablauf des Deep-Water-Horizon-Unglücks am 20. April 2010 ist hinlänglich bekannt. Beim Abbau der Macondo-Bohrstelle im Golf von Mexico kam es zu einem Gasausbruch, der die zugehörige Bohrinsel in Brand setzt. Elf Besatzungsmitglieder fanden den Tod. In der Folge kam es zu einem Austritt von Gas und Rohöl am Meeresboden in ca. 1600 m Tiefe, der 87 Tage anhielt. Er hätte verhindert werden sollen durch einen sogenannten Blow-out-Preventer (BOP), eine Schutzeinrichtung am Meeresgrund. Ihre Aufgabe wäre es gewesen, die Bohrleitung mit Hilfe eines hydrauli-

schen Mechanismus zu durchtrennen und zu verschließen (sog. Blind-Shear-Ram). Durch die Zerstörung der Bohrinsel und die Beendigung der Kommunikation zwischen ihr und dem Blow-Out-Preventer waren die Bedingungen für das Auslösen des Blind-Shear-Rams erfüllt. Zur Energieversorgung waren Hydraulik-Tanks auf dem Meeresgrund vorgesehen, die Steuerung war doppelkanalig ausgelegt. Die eine Einheit wurde „Yellow Pod“ genannt, die andere, gleichartige „Blue Pod“.

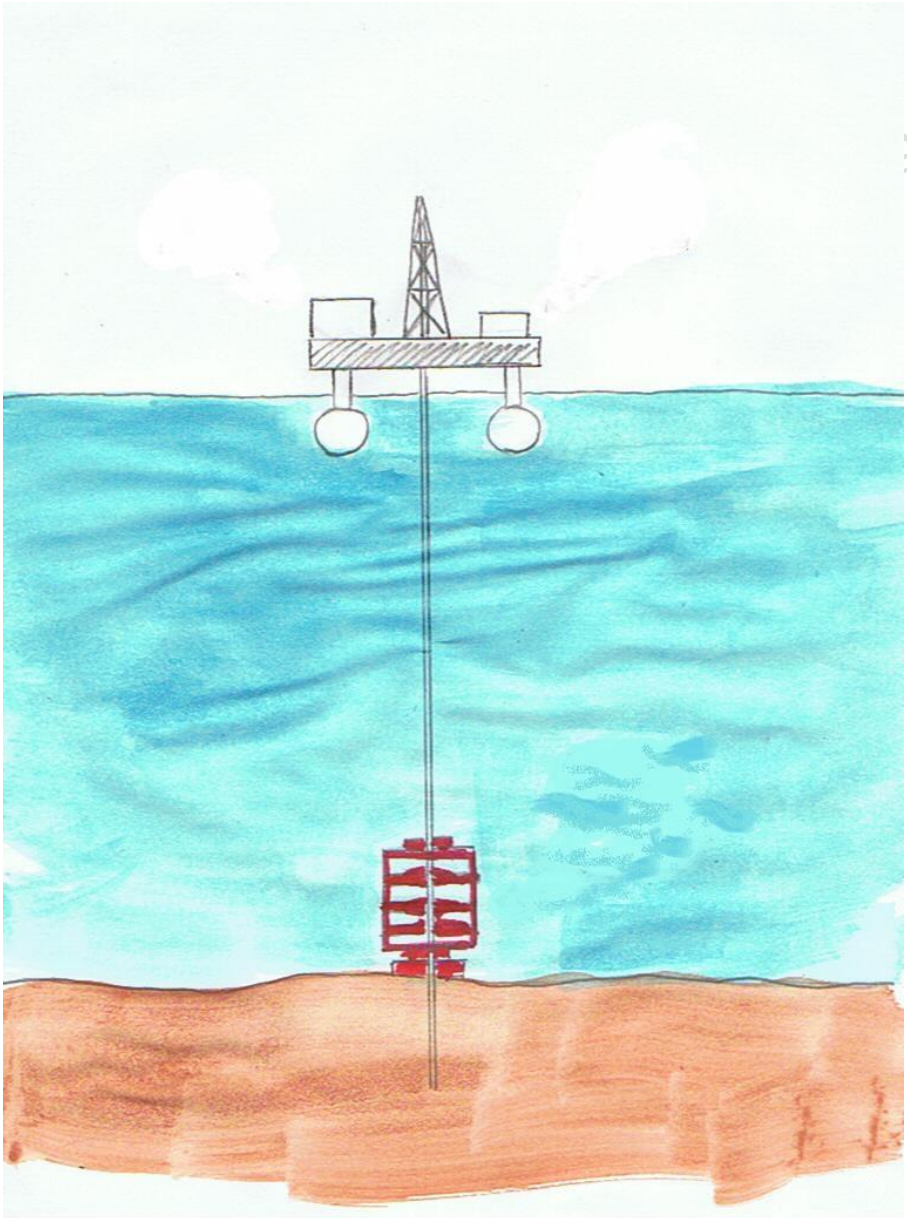

Abb. 1.3: Schutzeinrichtung zur Unterbindung eines Gas- und Rohölausbruchs am Meeresgrund, sog Blow-Out-Preventer (BOP)