Learning for safety in health care and air traffic control

Ternov, Sven

2011

Learning for safety in health care and air traffic control

Sven Ternov

Learning for safety in health care and air traffic control.

Doctoral thesis at Lund University

ISBN 978-91-7473-118-7
ISRN LUTMDN/TMAT – 1023 – SE
ISSN 1650 – 9773 Publication 41

Printed by Mediatryck, Lund, Sweden.

Table of Contents

Acknowledgements

Thank you to all operators in both health care and air traffic control.

The people at “the sharp end” in paper I saw me as a regulator official, and so I was. In spite of this they offered me their trust during interviews, and made it possible for me to unravel the twists and bends that ultimately lead to disaster.

The air traffic controllers at Malmoe air traffic control centre showed a marvellous ability to convey to me the secrets of air traffic control, and were willingly discussing the many “odd” questions I put to them. They eagerly participated in the discussions enabling paper II. Also they trusted me and cooperated when completing paper III.
During that time I was given excellent support from the site manager, Alf Månsson.

The National Board of Health and Welfare has enabled this thesis by allowing me to participate in courses on quality control and quality management. This was, at that time, not mainstream at the Authority, but my superior, the late Holger Hansson, had full trust in me. My next superior at the Authority, Ulla Fryksmark, supported my views on conducting MTO-analyses, and we had a lot of fruitful discussions. She could have turned me down as this approach was hardly accepted by the nomenclatura at the Authority, but she showed the courage and foresight not to do so.

My principal supervisor, senior professor Roland Akselsson, at the Lund Institute of Technology, took me “under his wing” and made me a PhD student at the institution. At that time I had tried to interest the medical faculty in my ideas, but alas totally in vain. Without professor Akselsson’s support I would never have set out on this long journey.
Professor Akselsson taught me the basics of scientific thinking, and, above all, instructed on the art of precision when writing a scientific article.

Åsa Ek, PhD, my assistant supervisor, has provided me most valuable feed-back and piloted me through the final works, criticising inconsistencies, pointing out ambiguous statements and assisted me in placing text under their proper headings.

Professor Akselsson introduced me to the Malmoe air traffic control centre.
My liaison there was Bengt-Inge Hallberg, at that time in charge of education, which was my means of introduction to the organisation. His never-ending support helped me a great deal in gaining the confidence of the controllers
As the work with paper II was concluded (with quite a few harsh remarks on the unit’s safety management system) he introduced me to the Luftfartsverket (LFV) HQ CEO, Michael Standard. He had the strength of mind to employ me, in spite of my criticisms.
And there I remained for a period of nine years, all the way to my eventual retirement.

As I never received any funding for doing this thesis, and as I had to earn my living at the same time as I was doing the research, things began to grind to a halt. Actually I had given up doing a PhD altogether.
Then a fellow researcher at the institution, AnnSofie Fyhr, a pharmacist, decided that I should get back on track, and put me in touch with a very dynamic associate professor at the institution, Sidney Dekker. He provided me with the necessary energy boost as well as knowledge on complex systems, which was the theoretical framework I needed for discussing the thesis.

Peter Andersson, Stabbarp Consulting, a former nuclear power plant control room engineer, introduced me to the management at a Swedish nuclear power plant and let me in to the mysteries of nuclear power. Thanks to Peter I got the opportunity. to do a DEB analysis for one of the processes necessary for starting up a nuclear reactor after the annual shut down and maintenance. Unfortunately this work remains as an internal report, not published in any scientific journal.
After a while we changed places, Peter now being “the new eyes” while I was the subject matter expert, when we did paper IV at a health care unit.

List of papers

Paper I
Ternov S, Akselsson R**. System weaknesses as contributing causes of accidents in health care.** International Journal for Quality in Health Care, Volume 17, Number 1: pp. 1–9 ,2005.

Paper II
Ternov S, Akselsson R. **A method, DEB analysis, for proactive risk analysis applied to air traffic control**. Safety Science 42:657–673, 2004.

Paper III
Ternov S, Tegenrot G, Akselsson R. **Operator-centred local error management in air traffic control.** Safety Science 42: 907–920, 2004.

Paper IV
Ternov S, Fyhr A, Akselsson R**. System weaknesses in the process of treating patients with cytotoxic drugs.** Draft**.**

Abbreviations

AIRPROX: As a general rule two passenger jets shall be separated from each other at least 1000 feet vertically and or 5 nautical miles laterally. Other separation minima can be in used close to airports.

Abstract

Introduction

Risk management in enterprises, organisations and companies has had a long and complicated history.
During the eighties, and at least during the beginning of the nineties, the notion concerning risk management was that if an accident happened in an otherwise perfect system it was due to the human operator in some way being the cause of the error. The cause for the accidents was described in terms of "negligence", "lack of competence" and such similar statements.

Gradually, during the late nineties, the risk management paradigm shifted.
James Reason, a psychologist, made a tremendous impact with his book *Human error*, published in 1990.
He introduced the term *latent failures* (or *latent conditions*). These, he said, are "resident pathogens", built into the system. They are latent since the system can live with these pathogens for months and even years, and perform adequately, until something happens, which hampers the "immune system of the system".
Reason states that the human operator goes to work everyday with the intention of doing a good job. The human operator has no wish "to screw up things". When accidents happen, and operators make mistakes, it is therefore not a deliberate action. The causes should be sought in design flaws in the system.

In this thesis we are dealing with high-risk systems, though not high-risk technologies. We are studying acute somatic health care, air traffic control, pharmacy and cancer treatment. We will explore different ways for an organisation to receive feedback from safety related occurrences, in order to improve safety.

The aim with this thesis will be to explore methods for obtaining safety feedback in the above mentioned domains.
Four different approaches will be attempted:

- Retrospective learning from accidents (paper I)
- Proactive learning using an external agent (paper II)

- Operator centred learning (paper III)
- User centred proactive learning (paper IV)

Methods and material

Methods

In paper I we used MTO (Man-Technique-Organisation) analysis as described by the nuclear power operators in Sweden, with a certain adaptation for health care.

Paper II was inspired on the work with paper I. During the numerous interviews with doctors and nurses a quite common reaction was: "Why did we not think of these risks before? It is so obvious!"
Another concern was the limited value of retrospective investigations when it comes to improving safety.
This started us on designing a method for proactive risk analysis. Several methods were already described for this, but they were mainly tuned to technical systems with more or less tight coupling, assuming a high degree of linearity (as for instance the Failure Mode and Effect Analysis, FMEA). We felt these methods did not fit the way in which our studied organisations functioned. The result was the DEB (Disturbance- Effect-Barrier) analysis used in paper II. The identified system weaknesses by using this method was compared to system weaknesses extracted from the analysis (done by headquarter analysts) of 15 loss of separation incidents at the unit.

When working with this it became obvious that one category of incidents, i.e. the loss of separation incidents (AIRPROX) , was only the tip of the iceberg. Each day there were a number of near misses that did not result in loss of separation, and therefore not used for safety feedback. Talking to the controllers also revealed a hidden knowledge on questionable procedures that might constitute risks. Thus the idea was fairly simple: Why not let the controllers do the job of analysing safety occurrences? This led to the design of a method for operator-centred learning, i.e. paper III. The method included a brief to the controllers for 1½ days on system thinking.

The starting point for paper IV was particularly tragic. I investigated a case where an eight-year-old girl with cancer was killed by mistake. She was administered the total dose of

cytotoxic agents each day for three days, i.e. a 300% overdose. We used the DEB analysis again, for a proactive risk analysis of the process of treating patients with cytotoxic drugs, but this time using a formalised user group.

Material

The material for paper I was a consecutive series of eight reports to the National Board of Health and Welfare, from acute somatic health care.

The material for paper II was a DEB analysis performed for the processes at the Malmoe air traffic control unit in Sweden.

In paper III a trial was performed for half a year with extended reporting of learning occurrences. In this way an additional 45 occurrences were reported which otherwise would not have been documented and analysed.

In paper IV the DEB analysis were performed at one ward unit at the department of oncology at the Lund University hospital, taking into consideration interface problems between the ward unit and the hospital pharmacy (which prepared the cytotoxic infusions).

Results

In paper I we could demonstrate that the notion of latent conditions was fruitful for analysing and learning from medical accidents. We identified a number of system weaknesses in seven out of eight cases, providing a good potential for improving safety.

In paper II we identified a number of risks (latent conditions) in the air traffic control system. We compared the identified system weaknesses with 15 loss of separation cases, investigated by the regulator. We identified all system weaknesses from 14 out of 15 as loss of separation analyses.

In paper III we could demonstrate that the operators indeed were able to analyse “learning occurrences”, and to identify preventive actions, one of these being training on the aircraft flight management system for controllers. Also, they could show that quite a few number of “unexpected flight behaviours” actually were actually partly caused by air traffic control actions.

In paper IV we refined the DEB analysis by using a formalised reference group of staff from the very beginning.. The analysis disclosed a number of system weaknesses, which were presented for the staff. The disclosed risks were accepted as valid, and quite a few of our recommendations were implemented during the next couple of years

Discussion

We discuss our methods in relation to current research, particularly we discuss MTO analysis in relation to root cause analysis, and DEB analysis in relation to FMEA. We are critical to both. We find that both methods could benefit from using the notion of latent conditions, and even applying the concept and vocabulary from the ISO 9000 quality management standard when describing risks.

We discuss the learning potential of retrospective vs. proactive analysis and are in favour of proactive methods.

We introduce complexity theory and relate this to our results. Our conclusion is that the operator-centred approach (paper III) seems to be the most effective way of influencing a complex system in a desirable manner, concerning self-organising and emergent properties.

Abstract in Swedish

Hantering av risker i företag och organisationer har haft en lång och komplicerad historia. På åttiotalet, och i början av nittiotalet, var uppfattningen att om en olycka inträffade i en organisation, som påstods vara nära nog perfekt, måste det bero på ”den mänskliga faktorn”, dvs. att en eller flera medarbetare inte gjorde som de borde ha gjort. Orsakerna till olyckan beskrevs i termer av försumlighet, bristfällig kompetens och slarv.

Synen på riskhantering ändrades så småningom på sent nittiotal. James Reason, en psykolog vid University of Manchester, fick stor genomslagskraft med sin bok ”*Human error*”. Han introducerade begreppet ”latenta fel” (eller ”latenta förhållanden”). Dessa latenta fel, menade han, var ”sjukdomsalstrare”, inbyggt i produktionssystemen. Ett produktionssystem kan leva med dessa länge, tills något händer som stör produktionssystemets ”immunsystem”. En jämförelse från det medicinska området är att våra kroppar härbärgerar många potentiellt farliga mikroorganismer, men de hålls i schack av andra mikroorganismer och vårt immunsystem som utgörs av olika vita blodkroppar. Om vårt immunsystem slås ut, som t.ex vid cellgiftsbehandling, blir dessa bakterier plötsligt väldigt farliga för vår hälsa.

På samma sätt kan oförutsedda händelser inträffa i ett produktionssystem. Ett antal latenta fel byter skepnad från att vara latenta till i högsta grad aktiva, och kan orsaka en olycka.

Reason säger att människan i systemet, medarbetaren, går till arbetet varje dag med ambitionen att göra ett bra jobb. Medarbetaren går inte till jobbet med målsättningen att orsaka en olycka. När därför olyckor inträffar för att medarbetare gör fel, är det inte för att medarbetaren avsiktligt har gjort ett fel. Det är snarare så att medarbetaren har fångats i en ”felfälla” pga. brister i utformningen av produktionssystemet.

Denna avhandling rör högrisksystem, men inte högriskteknologi . Vi undersöker akut somatisk sjukvård, flygtrafikledning, apotek och en cancerklinik. Vi vill undersöka olika sätt för en organisation att få återkoppling från inträffade händelser/olyckor så att den kan lära av dessa, och förhoppningsvis förbättra säkerheten.

Målet för avhandlingen är att undersöka olika sätt att åstadkomma denna återkoppling på, samt att reflektera över om några av dessa sätt är bättre än andra när det gäller att få en organisationen att dra nytta av informationen.

Vi vill pröva fyra olika tillvägagångssätt för att inhämta information om risker:

- Retrospektivt lärande från inträffade händelser/olyckor (paper I)
- Proaktivt lärande, dvs. få information om risker i systemet utan att vänta på att en olycka skall avslöja riskerna. Här använder vi en expert för att göra analysen (paper II)
- Operatörscentrerat lärande. Här låter vi ”folk på golvet” stå för datainsamling och analys (paper III)
- Användarcentrerat proaktivt lärande. Analysmetoden är den samma som i paper II, men med den skillnaden att vi använder en referensgrupp som består av ”folk på golvet”, dvs. det blir mindre av expertinflytande och mer av medarbetarinflytande under analysens gång (paper IV).

Metoder och material

Metoder

I paper I använde vi MTO (Människa-Teknik-Organisation) analys som beskrivits av kärnkraftsoperatörer i Sverige. Dock gjorde vi en viss anpassning från kärnkraft till sjukvård.

Paper II var inspirerat av arbetet med paper I. Vid de talrika intervjuer med läkare och sköterskor som genomfördes i paper I var en återkommande reaktion: ”Varför tänkte vi inte på dessa risker innan olyckan? Det är ju så tydligt.”
En annan reflektion var att retrospektiva riskanalyser kan vara bra för att förhindra en liknande olycka men att sannolikheten för att detta skulle inträffa, med exakt de samma förtecken, är minimal (jfr Tage Danielssons monolog om Harrisburg (Three Mile Island): ”Det kanske var bra det som hände i Harrisburg, fast det var osannolikt, men nu kan det osannolika inte hända i Harrisburg… igen”).

Detta fick oss att börja designa en metod för proaktiv riskanalys. Åtskilliga metoder för detta hade redan publicerats men dessa var i huvudsak inriktade på tekniska system, och förutsatte en hög grad av linearitet (om A inträffar, så inträffar med stor sannolikhet B och sedan C). Vi tyckte inte att dessa metoder var applicerbara på de organisationer som var i fokus för vår forskning (sjukvård, flygtrafikledning). Dessa fungerade i högsta grad icke-linjärt, eller komplext. Resultatet var DEB (Disturbance-Effect-Barrier) analysen som användes i paper II. Med denna metod hittade vi ett antal systemsvagheter (latenta fel och bristfälliga säkerhetsbarriärer) som vi jämförde med systemsvagheter som framgick av den centrala utredningsavdelnings analys av 15 fall av separationsunderskridande[1].

Under arbetet med paper II fick vi klart för oss att händelser med separationsunderskridande (AIRPROX) endast utgjorde en liten del av den information som kunde användas för att öka säkerheten. Regelbundet ägde händelser rum som var ”nära händelser”, dvs. en mer eller mindre okontrollerad situation som upptäcktes i tid så att händelsen inte utvecklades till ett separationsunderskridande. Vi uppfattade således att AIRPROX - händelser var ”toppen av isberget” och funderade på hur vi kunde komma åt en del av resten av isberget. Genom samtal

[1] Ett separationsunderskridande innebär att två flygplan har varit närmare varandra än 5 nautiska mil (NM) i sidled, eller 300 fot vertikalt.

med flygtrafikledarna upplevde vi att de hade en stor ”dold” kunskap om potentiellt riskfyllda rutiner och procedurer. Ur dessa iakttagelser kläcktes följande idé: Varför inte låta flygtrafikledarna själva stå för analysen av säkerhetsrelaterade händelser? Vi utvecklade därför en metod för operatörscentrerat lärande (paper III). I metoden ingick utbildning av flygledarna i ”systemtänk” om 1½ dag, samt formulering av vilka säkerhetsrelaterade händelser (utöver AIRPROX) de skulle rapportera och analysera.

Utgångspunkten för paper IV var tragisk. Författaren till denna avhandling utredde ett fall där en åtta år gammal flicka miste livet. Hon hade cancer, och fick av misstag totaldosen av ett cellgift varje dag i tre dagar, således en överdosering med 300 %.

Kliniken bad oss göra en proaktiv riskanalys. Vi använde DEB - analysen igen, på processen ”att behandla patienter med cellgifter”. Denna gång använde vi en formaliserad referensgrupp av läkare och sjuksköterskor, utsedda av kliniken.

Material

Materialet till paper I var en konsekutiv serie av rapporter (så kallade Lex Maria-anmälningar) till Socialstyrelsen i Malmö, från akut somatisk vård.

Underlaget för paper II var en DEB - analys av flygtrafikledningsprocessen vid *Malmö Air Traffic Control Centre (ATCC Malmoe).*

Materialet för paper III var en utökad rapportering av säkerhetsrelaterade händelser under en sex månaders försöksperiod. Under perioden rapporterades 45 händelser som annars inte skulle ha dokumenterats och analyserats.

I paper IV gjorde vi en DEB - analys av risker vid behandling av patienter med cellgifter, vid en vårdenhet på onkologiska kliniken, Lunds universitetssjukhus. I analysen ingick även analys av gränssnittsproblem mellan kliniken och sjukhusapoteket (som tillverkar infusionspåsarna med cellgifter).

Resultat

I paper I visade vi att det var givande att använda idén om latenta fel/latenta förhållanden för analys och lärande från olyckor i sjukvården. I sju av de åtta analyserade händelserna hittade vi risker i form av inbäddade latenta fel som det var möjligt att åtgärda.

I paper II identifierade vi ett antal risker (latenta fel) i ett flygtrafikledningssystem med DEB - analys . Vi jämförde våra resultat med de latenta fel som framgick av 15 fall av AIRPROX, utredd av tillsynsmyndigheten (Luftfartsverket). DEB - analysen identifierade 14 av de 15 systembrister som framgick av AIRPROX utredningarna.

I paper III visade vi att flygledarna mycket väl kunde analysera ”lärande händelser” och föreslå preventiva åtgärder. En sådan preventiv åtgärd var behov av att utbilda flygledare i hur ett flygplans autopilot ”tänkte”. Ett annat resultat var att ganska många fall där flygplanet gjorde något oväntat, och som traditionellt av flygledarna hade betecknats som SBS (”Skit Bakom Spakarna”) faktiskt visade sig delvis ha orsakats av flygtrafikledningen, och alltså inte bara var *flight deck error*.

I paper IV förfinade vi DEB - analysen genom att från första början luta oss mot en formaliserad referensgrupp av läkare och sjuksköterskor från kliniken. Analysen visade på ett antal systemsvagheter/risker. Detta presenterades för medarbetarna vid ett möte och accepterades som förståndigt (en korridorskommentar efter mötet: ”Det var en bra sågning”!). En stor del av våra förbättringsförslag implementerades sedan.

Diskussion

Vi diskuterar våra metoder utifrån det aktuella forskningsläget, i synnerhet diskuterar vi MTO - analys i relation till *root cause analysis*, och DEB - analys i relation till *FMEA (Failure Mode and Effect Analysis).* Vi är tämligen kritiska till båda. Vi menar att båda dessa metoder kunde förbättras och ge bättre resultat om man dels använde ”latenta förhållande konceptet”, dels tillämpade vokabulär och koncept från ISO 9000 - standarden för kvalitetsledningssystem.

Vi diskuterar potentialen för lärande för retrospektiva och proaktiva metoder och rekommenderar proaktiva metoder, såsom DEB - analysen.

Vi introducerar komplexitetsteori och relaterar denna till våra resultat. Vår konklusion är att den operatörscentrerade metoden (paper III) tycks vara den mest effektiva metoden för att påverka ett komplext system vad gäller systemets förmåga till självorganisering och önskvärda framväxande egenskaper (*emergent properties*).

Introduction

Risk management in enterprises, organisations and companies has a long and twisted history. During the eighties, and at least during the beginning of the nineties, the notion concerning risk management was that if an accident happened in an otherwise perfect system it was due to that the human operator in some way failed. The cause for the accidents was described in terms of "negligence", "lack of competence", "an air traffic controller is not permitted to forget", "carelessness", "lack of responsibility", "failure of performing the duties in an orderly way" etc.

The modern view, or let us call it a paradigm, is not old. As late as 1994 Marilyn Sue Bogner, from the US Food and Drug Administration compiled an anthology, *Human error in medicine*, with such distinguished scholars as Lucian L. Leape, Harold van Cott, Thomas B. Sheridan, David M. Gaba, Robert L. Helmreich, Richard I. Cook and David D. Woods and Jens Rasmussen[1]

Charles L. Bosk, a sociologist having studied the field of medicine, published his book *Forgive and remember* [2] as early as 1979.

Gradually, during the late nineties, the risk management paradigm shifted.
James Reason, a psychologist, made a tremendous impact with his book *Human error*, published in 1990[3]. It took some years, however, before his message was fully comprehended. What did James Reason say that changed the paradigm?

According to him accidents are due to system design flaws, which he labels "latent conditions" or "latent failures". The latent failures are, according to Reason, "resident pathogens", built into the system. They are latent since the system can live with these pathogens for months and years, and performing adequately, until something happens which hampers the "immune system of the system", to remain in the medical metaphor, making the pathogens virulent and causing disease, i.e. an accident. What hampers the immune system of

the system, i.e. the system's tolerance for unsafe behaviour is often labelled "situational factors", meaning contextual circumstances, which are impossible to predict.
Examples can be the combination of extreme pressure on an emergency ward unit due to major holidays, the introduction of a new computer system for handling patients and a stressed ambulance driver delivering a patient to the emergency department.
Or in air traffic control, as in the Überlingen midair collision disaster, the unavailability of a crucial safety net (short term conflict alert) and brake down of telephone communications.
Reason underlines that the mechanisms causing accidents are complex, not just one design flaw.

What Reason said was that the human operator goes to work everyday with the intention of doing a good job. The human operator has no wish "to screw up things". When accidents happen, and operators make mistakes, it is not deliberate but due to design flaws in the system. These design flaws "trap" the operator into making mistakes.
Therefore, to blame the operator will not contribute to enhanced safety. Instead one should try to understand the context of the accident, and identify what led the operator into making a mistake.

Reason acquired great popularity, perhaps because his message was somewhat global in nature, and he expressed himself in easily understandable language, accessible even to non-academics.

However, several other distinguished scientists contributed to the shift of paradigm from blaming the operator to looking for "system failures". Below are some of those mentioned.

A good example of the complex interactions leading to accidents is the disaster with the Challenger space shuttle. It exploded 73 seconds after take-off in 1986.
Diane Vaughan describes this in her book *The Challenger Launch Decision*[4]. There was a confusion of misunderstandings, misreadings, subtle (but dangerous) slides in company culture and inadequate chains of command.

> Its sources were neither extraordinary nor necessarily peculiar to NASA…Instead , its origins were in routine and taken-for granted aspects of organizational life that created a way of seeing that was simultaneously a way of not seeing.[5]

Sidney Dekker, In his *Field guide to human error*, starts with discussing the bad apple notion, i.e. if it were not for the bad apples no accidents would take place. If we get rid of the bad apples we improve safety.[6] This is contrary to modern risk management, he says. If we only get rid of staff that committed mistakes, instead of analysing the system for "design flaws", safety will not be improved, according to Dekker.

Dekker talks of "The new view on human error". However, he places a big question mark on whether "human error" is an appropriate term at all:

> : …a convenient but misleading explanatory construct.

Anyhow, this "new view" Dekker summarizes in three bullet points:

- Human error is not a cause of failure. Human error is the effect, or symptom, of deeper trouble.
- Human error is not random. It is systematically connected to features of people's tools, tasks and operating environment.
- Human error is not the conclusion of an investigation. It is the starting point.[7]

Bullet #2 is close to Reason's latent failures.

In Perrow's book entitled *Normal accidents*[8] he describes amongst other incidents "the normal accident" at Three Mile Island nuclear reactor. His focus is on high-risk technical systems such as nuclear power production, petrochemical plants, and air and sea transport. His argument for using the term "normal accidents", he says, is very simple:

> We start with a plant, airplane, ship…with a lot of components (parts, procedures, operators). Then we need two or more failures among components that interact in some unexpected way. No one dreamed that when X failed, Y would also be out of order and the two failures would interact so as to both start a fire and silence the fire alarm[9].

After this the plant may decide to install an additional fire alarm, and additional fire suppressing systems, which allows further unexpected interactions to occur.
This phenomenon Perrow calls the "interactive complexity" of the system. If this interactive complexity is combined with what he calls "tight coupling" recovery is not possible. What he means by this is that processes in such a system happen very fast one after another, and cannot be turned off. The initial disturbance will spread quickly and irretrievably.

In his book *Limits of safety* Sagan is concerned with the safety of the US strategically nuclear forces.[10]

He discusses two theories, high reliability theory and Perrow's normal accidents theory. He means that historical evidence provides much stronger support for normal accident theory, and he is more pessimistic than Perrow concerning the limits to organizational learning, i.e. that an organisation learns from mistakes in order to prevent new mistakes.
He lists some reasons for this. One he calls "the dark side of discipline". Military staff (handling nuclear weapons) lives in "total institutions". Apart from the official goals there are hidden goals such as to protect the institution from the outside world. This can encourage excessive loyalty and secrecy, and result in cover-ups of safety incidents.

> The root of the problem was more political in nature: strong disincentives existed against exposing serious failures. This influenced the reporting of near-accidents by operators…[11]

A main theme for this thesis concentrates on how people within an organisation can improve their awareness of risks when they carry out their duties, thereby improving safety.
One way is to learn from occurred accidents, incidents, near misses etc. (these terms often mean different things to different authors), so as to prevent similar occurrences.

Koornneef[12] in his thesis focuses on learning from what he calls "small-scale incidents" and "surprises".

Reason[13] points out the necessity for collecting data for such occurrences and points out that for this data collection to happen an "informed culture" in the organisation is a necessity.
Ek[14], in her thesis, deals with different dimensions of organisational safety culture, and discusses learning in relation to this.

In this thesis we are dealing with high-risk systems, though not high-risk technologies. We are studying acute somatic health care, air traffic control, pharmacy and cancer treatment.
We will explore different ways for an organisation to obtain feedback from safety related occurrences, in order to improve safety.

The aim of this thesis will be to explore methods for receiving safety feedback in the above-mentioned domains.
Four different approaches will be attempted:

- Retrospective learning from accidents (paper I)
- Proactive learning using an external agent (paper II)
- Operator centred learning (paper III)
- User centred proactive learning (paper IV)

A general problem with reporting systems, in order to learn about the risks in a system, is the degree of the operators awareness of risk. With a low degree of risk awareness only rather salient occurrences will be reported. With a higher degree of risk awareness operators may start to report occurrences where ‘‘nothing actually happened but there was a risk that something could have happened”.
This topic is, amongst others, discussed in an article *Learning from accidents – What more do we need to know*, by Lindberg, Hansson and Rollenhagen[15]. In it they make a comprehensive meta-analysis on the topic of retrospective learning.

We will compare and discuss the suitability of the different approaches for increasing risk awareness within an organisation.

Emergent research strategy

The research strategy for this thesis developed gradually over time. When thinking about paper I the author had no idea that he was going to design and try a proactive method for risk analysis (DEB), and had definitely no plan of applying it on air traffic control.

Spending quite a lot of time with controllers resulted in the idea for paper III.

The story could have ended here, if the department of oncology had not started to discuss medication risks with the hospital pharmacy. A pharmacist here (co-author to paper IV) knew I was working on a proactive risk assessment method. So I was given the possibility of finally trying the method in a health care setting (which was the intention from the onset).

Below I will attempt to describe this "research journey" in greater detail.

Paper I

As this thesis has been under way for quite a long time safety paradigms have changed. The context for writing paper I was due to my being employed as a medical supervisor at the National Board of Health and Welfare in Sweden. My job was to investigate medical accidents (iatrogenic), reported to the authority.

There was a strong tradition at the authority to hunt and punish "scapegoats", supported by a very counterproductive legislation (if safety matters). The National Board was top heavy with law-educated people and to these it was obvious that somebody had to be blamed for an accident. There was, however, a loophole in the legislation. If "other circumstances" could be demonstrated the committed faulty act might be "excusable".

At that time there was a, (at least orally) shift of paradigm. Somebody at the Authority had read about having a system's view on accidents. Thus we (the investigators) should try to identify "systemic factors" for explaining the accidents, though very few in the management really knew what this meant, or believed in it.

We (the investigators) read Reason's work, and tried to apply his terms of latent failures and situational factors when investigating medical accidents.

We were searching for a proper method to use. Via contacts with the Swedish Nuclear Power Regulator (SKI) we learned about MTO (Man-Technique-Organisation) analysis, basically a straight forward linear model, where the analyst works his way backwards from the accident, trying to identify cause-effect relationships and thus disclosing "systemic factors".
Applying the MTO analysis worked out fine. We could in almost all cases identify a number of "excusable circumstances", and we were able to get the doctors and nurses involved "off the hook" of the Disciplinary Board.
However, our superiors were not in favour of this. To them this notion of "systemic causes" was means of cheating, with the sole aim of covering up for negligence. So, in short we did what we were told to do (finding "systemic causes") but when the "nomenclatura" saw the results they got very critical.
Thus, the aim with paper I was basically to demonstrate that health care was no different from other high-risk systems (a lot of people thought so, particularly doctors), that it indeed could be looked upon as a system, and that accidents could be investigated accordingly.

To day this may seem obvious and history, but this was not the cause 15 years ago.
Today, this shift of paradigm, from punishment of "culprits" to identifying systemic causes for accidents, has finally made a footprint in the legislation. The Disciplinary Board will, end of this year (2010), no longer occupy itself with this kind of activity.

Paper II

Paper II was inspired by the work completed on paper I. During the numerous interviews with doctors and nurses a quite common reaction was: "Why did we not think of these risks before? They are so obvious!"

Another concern was the limited value of retrospective investigations when it comes to improving safety. Accidents do often happen due to the unlucky marriage between some latent failures and some totally unforeseen triggering factors. The probability that this combination will ever happen again is negligible. Using and applying a strict definition of latent failures can partly reduce this problem. This will be further discussed in the section "Theoretical considerations".

These considerations started us on designing a method for proactive risk analysis. Several methods were already described for this, but they were mainly tuned to technical systems with more or less tight coupling, assuming a high degree of linearity. We felt these methods did not fit the way in which our studied organisations worked. They had, to use Perrow's words, a "high degree of interactive complexity", and were loosely coupled.

The result was the DEB (Disturbance- Effect-Barrier) analysis. Whilst we were pondering over where to put it into practice, the air traffic control centre at Malmoe airport turned to our department and wondered if we could help them. They were worried over a rather sharp increase in incidents. We offered to do a proactive analysis using the DEB-method, which they accepted. And this we did, which explains the reason for the switch from health care to air traffic control.

Paper III

Paper II was very much an "external expert" exercise. We performed the DEB analysis and informed the control centre where the problems lay.

Whilst working with this it became obvious that one category of incidents, i.e. the loss of separation incidents (AIRPROX)[2] , was only the tip of the iceberg. Daily there were a number of near misses, not resulting in loss of separation, and therefore not used for safety feedback. Talking to the controllers also revealed a hidden knowledge of questionable procedures that might constitute risks. Thus the idea was fairly simple: Why not let the controllers do the job analysing safety occurrences?

Management support was granted us for creating a local reporting system, called "learning occurrences".

The aim was:

- To make better use of the learning value from non-AIRPROX cases.
- To get a deeper and more systematic engagement of the controllers in the flight safety improvement process.

[2] AIRPROX: As a general rule two passenger jets shall be separated from each other at least 1000 feet vertically and or 5 nautical miles laterally. Other separation minima can be in used close to airports.

The study questions were formulated thus:

- What can be learned about how to market a reporting system for the controllers, and how to train them for performing the analyses?
- Is it possible to identify certain risk patterns from the reports?
- What can be learned about recovery from disturbances?
- Is expert support needed, and if so, when and how?
- Will the reporting system produce suggestions for concrete flight safety improvements?

Paper IV

With paper IV we once again returned to health care.

The starting point for this paper was very tragic. I had investigated a case where an eight-year-old girl with cancer was killed by mistake. She had been administered the total dose of a cytotoxic agent each day for three days, i.e. a 300% overdose.

The manager (co-author of paper IV) of the cytotoxic drug preparation unit at the university hospital contacted me and expressed certain safety concerns, above all interface problems involving cancer ward – pharmacy.

We received an assignment from the management of the department of oncology to conduct a proactive risk analysis.

We used the DEB analysis, but this time with a well defined user participation from the staff at the department (as compared to paper II).

The research aims were to identify latent failures and insufficient safety barriers for the processes at one oncological ward unit.

What made this study special was that the pharmacy had a barrier function for mistakes made at the ward unit, and, vice versa, the ward unit constituted a barrier against mistakes at the drug preparation unit.

The analysis team was multidisciplinary, consisting of a licensed doctor (corresponding author), a pharmacist (the co-author) and a nuclear control room engineer (more on this choice later).

Emergent research objectives

After this research journey the research objectives, in retrospect, turned out accordingly:

1. Is it possible to use Reason's notion of a systems view in health care, and thus identify latent failures and insufficient safety barriers?

2. To design a method for proactive risk analysis

3. To try out this method for identifying latent failures (and insufficient safety barriers)

4. Is it possible to increase awareness of risks for air traffic controllers by giving them responsibility for collecting and analysing "safety occurrences", i.e. increased user participation at the expense of expert dependency?

5. To perform a DEB analysis with a well defined and formalised user participation.

Pondering over these empirical studies gradually an overall research objective emerged: What were the pros and cons for these different approaches when it comes to influencing an organisation towards increased awareness of risks?

Four different approaches were tried:

- Retrospective learning from accidents (paper I)
- Proactive learning using an external agent (paper II)
- Operator centred learning from near misses (paper III)
- User centred proactive learning (paper IV)

Research settings

The research settings are threefold: Acute somatic health care, air traffic control, and specialised health care (cancer treatment) /pharmacy.

Acute somatic health care

Acute somatic health care includes transporting the patient to the hospital, i.e. ambulance care. The ambulance delivers the patients to the emergency department. At the emergency department doctors and nurses take care of the patient. Crucial information is exchanged (or ought to be) between ambulance personnel and emergency department staff. Where was the patient picked up? What were the circumstances? What were the vital signs of the patient on first contact? Which treatment did the ambulance staff administer?

At the emergency department it is essential to get a diagnosis quickly, so as to start the necessary treatment. Sometimes (hopefully) it is highly qualified doctors who examine the patient and assess which tests will have to be performed for establishing a diagnosis, including amongst other diagnostic measures different X-ray examinations, blood tests etc. Whilst collating the appropriate information necessary for paper I, it became apparent that it was mainly trainee doctors who would make the initial assessment of the patient. This is gradually changing in Sweden, concentrating acute care to fewer hospitals and subsequently putting qualified emergency doctors on the front line.

In terms of organisation the initial assessment of the patient is a challenging procedure . Knowledge from several medical specialities may be needed, which ultimately involves quite a lot of people. They will have to coordinate their efforts, under heavy time pressure, to agree on a diagnosis, and start proper and coordinated treatment. It may involve emergency care specialists, orthopaedic surgeons, abdominal surgeons, anaesthesiologists (intensive care) and internal medicine specialists.

To become a medical doctor in Sweden involves five years training in medical school, and a further two years to obtain a doctor's authorization, which allows the doctor to perform medical practice without supervision.

meaning that the doctor is allowed to perform work without supervision. For becoming a specialist an additional 4-5 years of training is needed. This rating is for life, with no additional requirements for training or proficiency checks.
This means that a doctor can be absent for several years, and then start to work again without any additional training. Nurses too get their authorization for life.

When something malfunctions in the treatment of a patient it can be called a lot of things. In Anglo-Saxon countries the term "adverse event" is frequently used, but rather ill defined. Does it mean that a patient was harmed, reversibly or irreversibly, or was the incident just a close call?

In Sweden the term "accident" is used for irreversible harm to a patient, including death. "Incident" is also used but can mean anything from reversible harm to a close call. A "deviation" includes the whole spectrum, from death to a near miss.
Where legislation is concerned a hospital must report to the regulator when a patient is harmed but even when there was a risk for harm to a patient This is regulated in an Act from the regulator, called "Lex Maria"[3]. [16]
Also, included in the same act is a requirement for local "deviation reporting". Here the terms "deviation", "negative event", "risk" and "harm to patient" is used. Unfortunately the terms are overlapping, and often difficult for hospital staff to understand.[17]

Air traffic control

The Air traffic control system guides aircraft during flight. Its main task is to avoid aircraft colliding. Basically air traffic flow is very regular from day to day. The aircraft follow "lanes" in the air. The surveillance is performed by radar, except when the aircraft is very close to its airport of destination or when taking off. Here the tower controller relies on visual monitoring of the aircraft.
The airspace is divided in a number of sectors, extending both laterally and vertically. Each sector has an assigned radio frequency, to which the aircraft radio is tuned. The pilots will listen to and follow instructions from the air traffic controllers, when to climb, when to

[3] Δ In 1936, at Maria hospital in Stockholm, four patients were injected with a disinfectant instead of an anaesthetic, and they died. Because no reporting system was in place the error was repeated four times before detected. Thus the Lex Maria Act was made.

descend and turn. The controllers issue these clearances after having analysed, minute for minute, the traffic situation on the radar screen.
An aircraft approaching an airport will have to descend through a lot of air, from 10 000 meters to ground level. The controller has to ensure that the descending aircraft does not come into conflict with aircraft flying below.

For communication purpose the controllers use radiotelephony to the aircraft, and interphone connections for coordinating actions between themselves (between different sectors). The processes involve a large amount of technical equipment (radar, radiotelephony, interphone, updating of flight plans, automatic exchange of information between neighbouring flight regions, communication with the central flow management unit in Brussels, computer based safety nets etc.).
The means of communicating between controllers and aircraft on the radio are strictly and internationally formalised, the so called “phraseology”.

In order to obtain a license to work as an air traffic controller requires three years of training. After this the controller can apply for a position as a controller, both in Sweden and internationally. After having acquired a position as a controller he/she must undergo additional training for approximately six months concerning the local airspace, before being allowed to work on his/her own. The rating is given by the regulatory body (in Sweden Transportstyrelsen). The rating is time limited. It must be renewed every 18 months. For renewal the controller must be able to document participation in additional training, amongst others training in a simulator involving irregularities, as well as a proficiency check. An additional requirement for getting a renewal of the rating is a minimum of working passes during the last three months period. If this is not met the controller will have to undergo additional training with a supervisor.

The controllers at the Malmoe air traffic control centre belong to one of three authorisation groups, depending on the type of airspace for which they have a rating, mainly approach (guiding and sequencing traffic to Copenhagen airport), Western en-route sectors and the Baltic Sea sectors.

One of the main tasks of the controller is to ensure that the "separation minima" is not violated. These minima are international requirements (ICAO[4]), and stipulate that an aircraft must never be closer to another aircraft than 1000 ft vertically and five nautical miles (NM) laterally. If these minima are violated it is a loss of separation incident, referred to as AIRPROX. It is mandatory to report AIRPROX incidents to the regulator.
During the last decade the development in Sweden concerning AIRPROX investigations has shifted from "go for the controller" to "go for system failures". This change of paradigm, however, has not come easily. The headquarters in particular has had difficulties in accepting this change. An effect of this is that the controllers have shown a reluctance to report anything more than is absolutely mandatory, thereby reducing the knowledge base for improving safety.
It should be mentioned that the difference between an AIRPROX and a near miss often depends on situational factors, out of reach for the controller. If a controller, for instance, suddenly realises that he has two aircraft on the same altitude, opposite each other, and evasive action is necessary, in one case the separation of 5NM may be maintained, in another the separation will be a violation with a lateral distance of for instance 4,8NM, and thus an AIRPROX. What constitutes the difference might have been different wind conditions, or the pilot in the first case reacting more quickly to controller command. But the learning potential and involved risks are equal, i.e. the controller missed a conflict between airplanes.

Oncology/pharmacy

Cancer treatment (discipline of oncology) is highly specialised. After having established the diagnosis of cancer the doctors has different options for treatments. These include surgery, radiation and treatment using cytotoxic drugs.

Treatment with cytotoxic drugs is mainly done by intravenous infusion, lasting from a couple of days to a week, and then repeated a number of times with a suitable interval in between.

The treatment is highly standardised, at least at the same unit of oncology. A combination of drugs is used according to a scheme. As a rule the aim is to give the patient a total dose of the drug during a treatment session. The dose is calculated from the scheme, amongst other

[4] International Civil Aviation Organization.

parameters taking into consideration the body mass of the patient and the kidney function (the drugs are mainly excreted via the kidneys, so an impaired kidney function may give too high a blood concentration of the drug (s) if the dose is not corrected according to the kidney function).

Between treatments a number of blood test have to be conducted, amongst other things the count of white blood cells. This is because most cytotoxic drugs have a depressing effect on the blood marrow (which create the blood cells). If the count of white blood cells, which is the base of the immune system, becomes too low the patient may die of an otherwise banal infection.

After having established the diagnosis the doctor chooses a cytotoxic drug “regime”. The prescription is handed over to the preparation unit at the pharmacy, which will prepare the infusion. A nurse at the cancer ward unit will administer the infusion to the patient.

The cancer ward and the pharmacy cooperate in quite a complex way, the one being a safety barrier for the other, in a two-way process.

Theoretical framework/considerations

On latent failures

We found Reason's latent failure (or latent conditions) concept fruitful, and has used it in all the papers. However, Reason is not particularly precise in giving a definition/explanation of the concept so as to facilitate its operative use during analysis. Therefore the following requirements were used for calling a finding a latent failure.

These were:

The identified risk must be expressed in a way that is independent of the operator.

Example: "The training of Dr. NN was insufficient for being on duty at the emergency department". This is not a latent failure.

However, this is: "The management at the department has not properly defined necessary competence for working at the emergency department".

By and large the operator at "the sharp end" cannot influence the identified risk, and

The identified risk can contribute to other accidents than one the studied.

Example: "When suspecting a case of appendicitis at the emergency department a senior doctor must examine the patient before he/she is discharged". This is not a latent failure; it is a specific statement for a specific case.

This, however, is a latent failure according to our definition: "The department does not have proper procedures to safeguard against a junior doctor making the wrong diagnosis and discharging the patient".

This last mentioned requirement is particularly important for avoiding that which was mentioned in the section "Introduction", that is that the analysis produces recommendations only for preventing a similar accident as the one being studied, bearing in mind that the probability that an accident with exact the same mechanisms will probably never happen again.

To give an example: During a heart catheterisation procedure it is customary to give the patient an intravenous infusion of nitroglycerin in order to stimulate the flow of blood. By mistake the patient was given adrenaline instead, which has the opposite effect. One cause for the mistake was that left over ampoules with adrenalin were stored together with ampoules of

nitroglycerin in the same box. So we could say that storage of adrenalin constituted a risk, a latent failure, which contributed to the mistake. To store adrenaline in a more appropriate way might prevent a similar mistake. This, however, does not fulfil the third requirement above, i.e.that the latent failure can contribute to other accidents than the one under review. The analysts should take a broader view and in this case ask whether this was typical when handling drugs in the operating theatre. This was actually the case, involving the careless handling of ampoules, labelling of syringes etc. Thus the "real" latent failure was "poor and inconsistent procedures for handling drugs".

We found the international standard for quality management, ISO 9000[18], most fruitful for providing a conceptual framework and a vocabulary for describing inconsistencies in the quality (safety) management system (which equals "latent conditions"), and for formulating corrective actions.
The manner in which the latent failures are formulated in the examples above is very much "ISO 9000 – inspired".

Another example can be seen in paper IV, "generic checklist".

Wiegmann and Shappell[19] have refined Reason's latent failure model by defining four "levels" of a production system, see illustration below, where latent failures may be identified for each level.

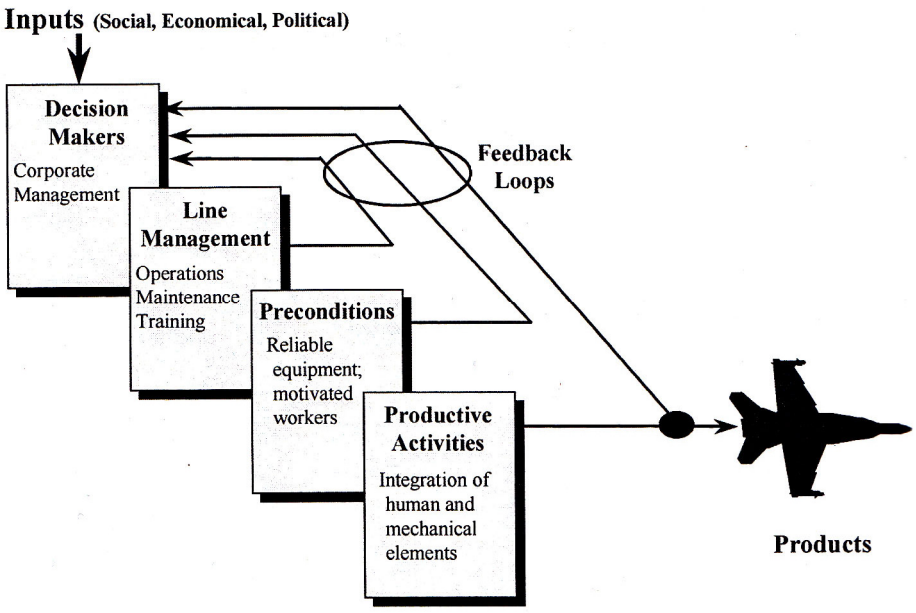

***Figure 1**. Wiegmann and Shappell's notion of levels in a production system, and the feedback loops between the levels concerning risks.*

They assume different feedback loops between the different levels.

Koorneef[20] has used the terms "first loop learning" and "second loop learning" which can be illustrated in the model of Wiegmann and Shappell. In "first loop learning" the organisation will adapt to input from for instance incident reports, and adjust its processes accordingly. This applies to the levels "Line management, preconditions and productive activities".
In "second loop learning" the organisation will adapt (change) its goals, which will take place on the level "Decision makers".

Wiegmann and Shappell elaborate further on their level model, see illustration below.

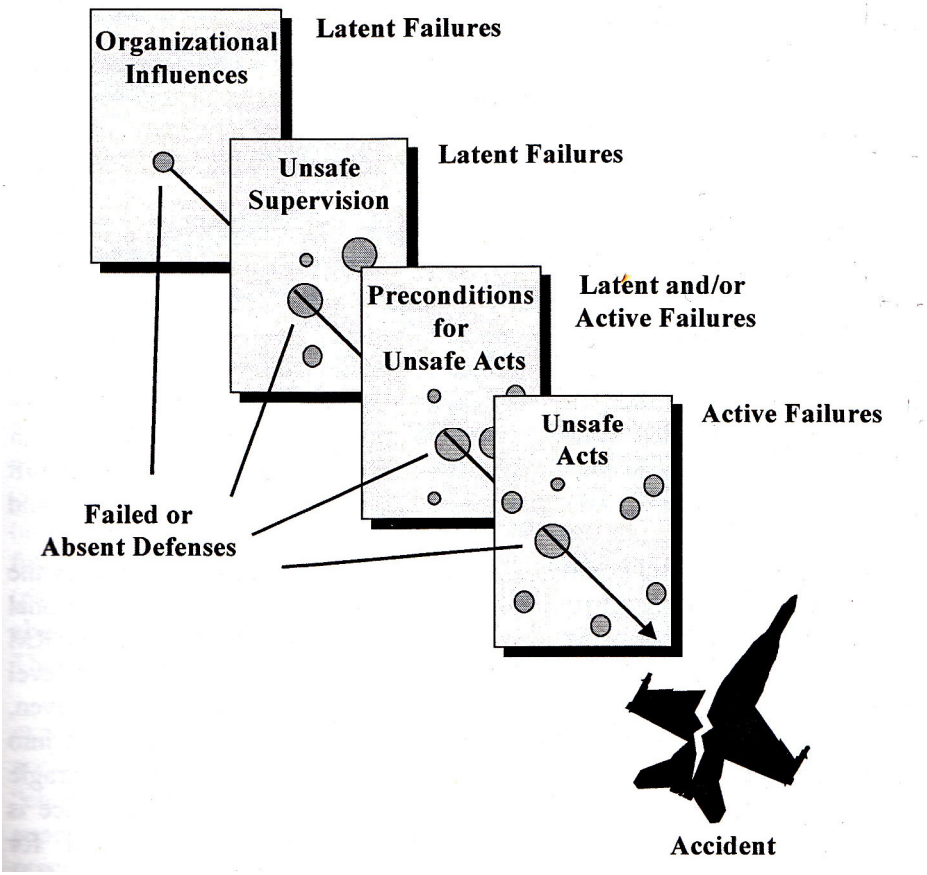

***Figure 2**. Wiegmann and Shappell's modification of Reason's "Swiss cheese model". They introduce three productions levels where latent failures can exis[21]t.*

Here they refine the Reason "Swiss cheese model" by defining different organisational levels for latent failures.

Wiegmann's and Shappell's model was anticipated by Rasmussen[22], in his "organisational level model", see illustration below.

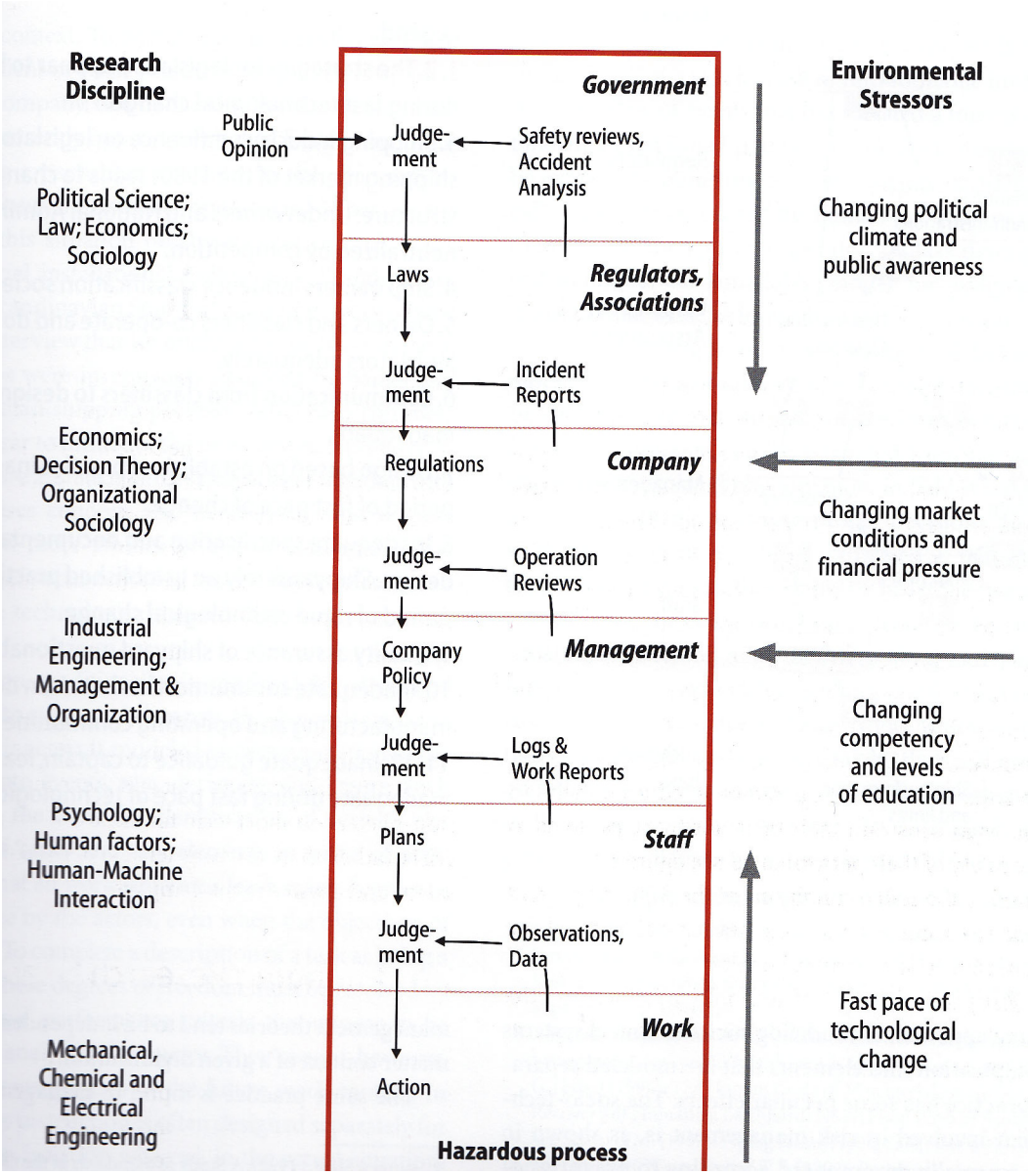

Figure 3. Rasmussen and Svedung's level model. It illustrates a complex interaction between multiple stakeholders.

In the text to this figure Rasmussen and Svedung write:

> …..This social organisation is subject to severe environmental pressure in a dynamic, competitive society. Low risk operations depend on proper co-ordination of decision making at

> all levels. However, each of the levels are often studied separately within different academic disciplines.

Rasmussen adds stakeholders that are outside the boundary of the company such as regulators, associations and government. He describes the environment requirements to the subsystems at the different levels (to which they will have to adapt), and he points out that to obtain operations with low risks will depend on proper coordination of decision-making at all levels, something which is more an exception than a rule.

On safety barriers

In all the papers we use the notion of safety barriers. We define this in paper I

> …as an administrative or technical constraint at operator level which will prevent an inappropriate human action, or absorb the effect of such an action, thus making the system "error tolerant" or forgiving.

This is further elaborated in[23] by Ternov in an anthology, *Error reduction in health care*, by Patricia Spath (ed.), and in Bosk: *Forgive and remember* [24].

Hollnagel has in his book *Barriers and Accident Prevention*[25] penetrated the notion of safety barriers in great detail.

His definition of a barrier is

> …An obstacle, an obstruction, or a hindrance that may either: (1) prevent an event form taking place, or (2) thwart or lessen the impact of the consequences if it happens nonetheless.[26]

According to Hollnagel, barriers that are intended to work before a specific initiating event takes place, serve as a means of *prevention*. Barriers that are intended to work after a specific initiating event has taken place serve as means of *protection*.

Hollnagel classify barriers into four categories: Physical barrier systems, functional barrier systems, symbolic barrier systems and incorporeal barrier systems.

He further presents eight dimensions for barriers for evaluating barrier quality, such as resource needs, reliability and dependence on humans.

In Hollnagel's terminology incorporeal barriers consist of rules and procedures to be followed and complied with. The reliability for these kind of barriers are generally low because they are dependent on an interpretation and compliance by the human operator.

On the other hand, physical barriers are not dependant on humans. They block or restrain harmful actions, independent of the operators' attitude to comply with rules and procedures. Thus they have a high reliability.

We use the terms "weak" and "strong" for safety barriers, where we claim that administrative barriers generally are weaker than technical barriers. Our administrative barriers correspond to Hollnagel's incorporeal barrier systems, and our technical barriers to Hollnagel's physical barrier systems.

In paper IV we further classify the strength of the safety barriers on a 1-5 scale.

Other research

Health care, retrospective methods

A search in the scientific database PubMed on "MTO analysis" and "safety" only retrieved paper I in this thesis.
A search for "Root cause analysis in health care" retrieved 21 articles.
Of these only four explicitly mentioned Root Cause Analysis (RCA).
In two of these articles RCA was used as a proactive method, one article mixing RCA with Failure Mode and Effect analysis (FMEA).
One of these four articles was actually a meta-analysis of RCA[27]. From a literature review this study concluded that there has been no controlled study that test the RCA framework, that RCA participants report difficulty in forming causal statements and in formulating corrective actions. Other criticisms include "the uncontrolled study design and participant biases".

The remainder of the articles comprised a wide spectrum of items, such as ab initio training and training of doctors, crew resource management, briefing-debriefing, generally about medical error, human factors engineering and quality improvement. It appears that RCA frequently is used as a concept, and not as a method, to demonstrate that authors have a "systems way of thinking".

13 of the retrieved 21 articles emanate from the US, the remainder from UK, Australia and Canada. Europe is represented by two articles only, from the UK (whatever the significance of that might be).

None of these articles contain a description of the method. However, a description was found in Vincent and Taylor-Adams: *Framework for analysing risk and safety in clinical medicine*[28], and also in [29], *How to investigate and analyse clinical incidents: Clinical Risk Unit and Association of Litigation and Risk Management protocol.*
The protocol complies with modern systems view. They refer to Reason and his latent condition concept, but for some reason they do not use it. Active failures they label "care management problems", which are rather misleading (it is not possible to know if an active failure was a "management problem" until after the analysis has been done).
The method in many respects resembles MTO analysis. A preliminary MTO analysis will be performed, and after that involved staff will be interviewed in order to complete the analysis.

In 2008 there appeared a "commentary" in JAMA (Journal of the American Medical Association) entitled *Effectiveness and Efficiency of Root Cause analysis in Medicine*.[30] It provides an interesting critical assessment of the use of RCA, concerning both a UK and a US perspective. The authors write that recommended actions such as redesigning a product or a process are strong and have a high probability of reducing harm, while recommendations such as re-training or writing a new policy, the two most common actions in the reviewed material, are weak and have a low probability of reducing risk. According to the authors many RCAs are performed incorrectly and do not produce usable results. Many organisations tend to misunderstand the method, by looking for the single "most fundamental reason". Overall, the authors conclude, the RCA analysts have difficulties formulating suggestions for corrective actions. The authors call for more cooperation between hospitals so as to aggregate information from RCAs, especially when it comes to design problems with devices. They write that many such problems are too big to be handled at hospital level.

Health care, proactive methods

A search in PubMed on "proactive risk assessment" gave 349 hits on a wide variety of subjects, though they were seldom linked to a method.

As the Failure Mode and Effect Analysis (FMEA) seems to be a widespread method, both in the UK and in the US, we searched for "FMEA in hospitals". This retrieved 35 publications, 24 from the US, 6 from UK, 4 from Italy and one from Australia.

Description of the method can be found in Spath: *Using failure mode and effect analysis to improve patient safety* [31]. In short the method consist of the following steps: Choose a sub process to be studied, assign a team, conduct a process analysis, for each step in the process determine possible ways the process could go wrong (labelled "failure modes"), for each failure mode determine the severity of the effect of the failure, determine the detectability of the failure, and, finally, determine the frequency of the failure. These last three steps are quantified on a 1-5 scale, and then multiplied to give a score governing which failure modes to prioritise for process re engineering.

In the retrieved articles FMEA was used on a wide range of clinical problems. Examples are quality of communication in emergency care, treatment of HIV in Swaziland, error reduction during patient-controlled analgesia therapy, reducing errors at a dialysis unit, error reduction in laboratory medicine, reducing inpatient suicide risks at a department of psychiatry, identifying risks when merging two hospitals, risks for processes in orthopaedic surgery, implementation of smart i.v. pump technology, and safe administration of chemotherapy to hospitalized children with cancer.

For all the papers the authors find that the use of FMEA gave them insights for reducing risks.

Three of these articles I would like to highlight; one article because it is the only one who contains a follow-up on recommended corrective actions, and the other two because authors conducted studies of the reliability of the FMEA.

The first article concerns chemotherapy to children[32]. The prescribing error rate was reduced from 23% to 14%, dispensing errors decreased from 3% to 1% and administration errors from 4% to 3%.

In the paper *Is failure mode and effect analysis reliable?*[33] the authors, emanating from the school of Pharmacy, University of London, let two FMEA teams analyse the same process, namely the administering process for two cytotoxic drugs, vancomycin and gentamycin. Each

group identified 50 potential failures, but only 17% of these they had in common, and they had very different risk priority numbers. The authors conclude that it is questionable to invest time and money for amending the identified risks, as long as the reliability of the results is so poor. They state, “health care organizations should not solely rely on FMEA to improve patient safety”.

Air traffic control, retrospective and proactive methods

Search in LibHub, the article database at Lund University, retrieved no articles, when searching for “risk analysis”, “MTO”, and “FMEA” in the title, and “air traffic control” as key word.

Methods and material

Method

In all four papers we use Reason's "latent failure" concept[34], though we use this concept with a stricter definition than Reason does. We even use the term "system weaknesses" = latent failures + insufficient safety barriers.

A facilitator for us in this respect has been to borrow the thinking and the vocabulary from the international standard for quality management, ISO 9000[35]. This has provided us with a good tool for expressing inconsistencies in a production system (the corresponding author is a trained auditor on the ISO 9000).

In our vocabulary a safety barrier is a constraint at the operator level, which reduces the degree of freedom for the operator, i.e. reduces the opportunity for the operator to make a wrong choice, or has the ability to mitigate the effect of an error.

In paper I the used method is MTO-analysis, as described by the Swedish nuclear power industry[36 37]. We modified and adapted the method for health care.
In the section "Discussion" below we discuss how our modified MTO analysis harmonise with complexity theory.

On proactive risk analysis, - developing the DEB analysis

As mentioned before a common reaction when interviewing staff during investigation of accidents (not only the eight used in paper I, but several hundred) was an insight that with some forethought a number of latent failures might have been possible to identify in advance. So we thought of how the MTO-analysis, used in paper I, could be "reverse-engineered". As for the MTO-analysis we wanted such a proactive method to be process-oriented and operator-centred. Also, we wanted to include items of the management quality system , ISO 9000, such as appropriateness of procedures and their implementation, clarity of roles, clarity of responsibility and handling of disturbances in the processes.

We wanted to stick to the latent failure concept and even wanted to include a safety barrier analysis. The argument for a safety barrier analysis was that when a latent failure was identified the risk could be managed in two ways (or in combination): either the latent failure could be eliminated, or a safety barrier engineered into the process.

A number of proactive methods had been described but none of these met our requirements. A key element in the DEB-analysis is the "what…if" question, that is, when we described what is supposed to take place during the different steps in a process (task analysis) we would ask "what if" process steps are not done as planned or intended? And what would the effect be? In this respect our method has similarities with the Action Error Method[38], but this method is mainly tuned for technical systems. The Failure Mode and Effect Analysis[39] is another proactive method, which as a starting point asked: How can this (technical) unit fail, and what would be the consequences?
A third method, the Hazard and Operability Studies (HAZOP)[40], also uses the "what…if" question, but for risks concerning the design of technical equipment.

An important issue for the HAZOP, as well for the DEB, is the use of reference groups. Doing the initial task analysis is mainly a desk job for the external agent/analyst, but when it comes to deciding upon the effect of disturbances during the different steps of the process we need staff involvement, and it is also very much needed when suggesting realistic safeguards /safety barriers. In paper II some trial and error was involved in doing this, in paper IV we managed to organize this in a much better way.

A further comment on "reversing" the MTO-analysis: The MTO analysis is basically linear in its approach. Knowing the outcome (the accident) to the MTO analysis backtrack the chain of events leading to the accident: NN made a wrong decision, YY did not detect the mistake and therefore XX did what he did, and it all went wrong.

In the DEB analysis complexity enters the scene When we for a certain step in the process ask "what could go wrong" it is fairly easy to come up with some suggestions, but when we ask: "what would happen, what would be the effect?" we actually do not know. A lot of things can happen, or nothing at all, depending on the actions of the operators (of which we cannot know) and circumstantial factors (which never can be foreseen). This is in contrast to a tightly coupled technical system as in process plant.

To give some simplified examples:
A radiologist makes a wrong interpretation of an X-ray. What will the effect be?
Maybe none at all, after all this investigation was not really important to the clinician (maybe the X-ray was ordered by a junior doctor, "just in case…").
Or an unnecessary operation was performed.
Or the clinician became suspicious and went to see the radiologist, and they detected the mistake together.
Or complementary investigations were performed, and the (wrong) diagnosis could not be verified.

A second example from paper II:
In air traffic control a flight progress strip (FPS) for each flight must be placed in a bay and will be moved in the bay according to the progress of the flight. This will assist the controller to update his/her mental picture of the traffic. A latent failure identified was that the use of FPS was insufficiently defined. Some controllers used it as intended, others less so. What would the effect be? We do not know. The only thing we could say is that it is a risk not to use FPS properly. Whether or not this risk turns into an accident depends on a lot of factors (on which we can only speculate).

A third example, also from paper II:
A controller gives an aircraft a new altitude in which to fly (flight level). The intention was correct, i.e. the new flight level was safe, but for some reason (interruption by another call, interruption from a fellow controller, or teacher student situation etc.) the controller clears the aircraft to another flight level than the one intended. What would the effect be? Worst case would be a midair collision.

Nothing would happen if there was no aircraft on the same flight level in the opposite direction. Maybe the aircraft would receive an alert from its on board alerting system (TCAS). Or a fellow controller might detect the mistake. Or the controller himself would detect it whilst doing his routine follow up scan of the traffic.

So, anything could happen, ranging from ultimate disaster to absolutely nothing. It is impossible to predict in such an interrelated system. But we can say that it involves a risk in

that there is no safeguard against the controller giving another flight level than the one he intended (such a safeguard is now, partly, implemented in a new air traffic control system ("System 2000")).

In paper II we use the DEB analysis (Disturbance- Effect-Barrier), and the method made its maiden voyage in this paper.

In paper III we defined a training curriculum for air traffic controllers for increasing their safety consciousness. We wanted to assess if this training would make them report safety occurrences beyond that which was mandatory to report.
A senior air traffic controller (co-author for this paper) gave support as a subject matter expert.

In paper IV we again used the DEB analysis, this time in a in a health care setting, but with a more formalised role for a reference group, compared to paper II.

Material

The material in paper I consists of eight consecutive reports to the regional regulator (National Board of Health and Welfare, regional unit in Malmoe, Sweden) according to the Lex Maria Act, concerning accidents in acute somatic health care.

The material in paper II is a DEB analysis performed at the air traffic control centre, Malmoe airport.

In paper III the material is extensive reporting of "safety occurrences" at the same air traffic control centre as above. It consisted of 44 reports during a six month trial period.

In paper IV the material is a DEB analysis performed at the department of oncology at the university hospital in Lund, Sweden.

Summary of papers

Paper I. System weaknesses as contributing causes of accidents in health care.

Basically the study question was: can a system's view be applied to accidents in health care, or is health care a stand alone enterprise, following totally other rules than other high risk systems? We demonstrated convincingly that a system's view was fruitful for analysing health care accidents. A suggestion to the National Board of Health and Welfare was, at least implicit: Please join us in the modern world of risk management. Now, six years after this paper was published the legislation has turned towards a modern understanding of accidents (of course not only due to this paper).

The MTO analysis method proved fruitful, at least when our own strict definition of latent failures was used. A number of latent failures could be identified, and they served as "excusable circumstances", getting the doctors and nurses off the hook of the disciplinary board.

We could demonstrate three kinds of different latent failures: Latent failures that create opportunities for mistakes, latent failures as hindrance for error mitigation, and latent failures that create such a mess of the work situation that an operator sooner or later would make a mistake.

The situational factors, the unlucky circumstances, were, as expected, impossible to foresee.

We had some ideas of user participation when performing MTO-analyses (apart from the interviews) and tried it out on other cases, but with no success. I think we underestimated the training need for health care staff, should they themselves do the analysis. However, in another setting and in another country, where the corresponding author was involved as trainer, it actually showed that health care staff indeed was able to learn to do MTO analysis, with relatively little supervision.

Paper II. A method, DEB analysis, for proactive risk analysis applied to air traffic control.

This study was the maiden voyage for the DEB analysis. The aim was to apply it in an air traffic control setting and to see if latent failures could be identified.

One might say that it was a very cumbersome way of testing a new method, going for a domain utterly unknown to the corresponding author (being a physician). It took at least half a year of hard work sitting in the "backseat", behind the controllers, to get a minimum of domain knowledge. Luckily (for me) the controllers were very keen and enthusiastic that somebody from the outside would learn about air traffic control, and they were good teachers.

When doing the analysis it was of a certain advantage to be an "outsider". I could innocently ask them questions which otherwise might have been taken as a criticism of their work. As it was, I was a strange bird in the control room, and thus not dangerous.

A positive side effect on doing the analysis in this domain was to realize that a method, inspired by health care, worked well for air traffic control as well.

In the study we wanted to assess the ability of the DEB analysis to identify latent failures. This was accomplished by comparing the result from the DEB analysis to earlier identified latent failures in a consecutive series of loss of separation (AIRPROX) incidents. The Swedish Civil Aviation Administration headquarters performed these incident investigations. The DEB analysis captured all latent failures from the AIRPROX incidents with exception of one. The reason for this was that the analyst (corresponding author) missed a sub process in the task analysis, namely the automatic sequencing system for arriving traffic to Copenhagen airport (MAESTRO).

As this was the maiden voyage for the DEB analysis there was, of course, a number of lessons learned when applying the method. The most important was that a formal reference group of staff should be appointed from the very beginning, helping the analyst with the task analysis, joining in with brainstorming sessions about possible disturbances and their effects, and facilitating the engineering of safety barriers.
We even experienced that proper "marketing" of the analysis was important. There was a tendency for controllers to "defend" their system.

Paper III. Operator-centred local error management in air traffic control.

The current reporting system focuses on shortcomings in methods and procedures and not on finding ‘‘scapegoats’’, according to the LFV manual for performing investigations. This centralised reporting system has, however, some drawbacks when it comes to its potential for improving flight safety:

1. The air traffic service units often reduce their role to only describing the incident, waiting for the headquarter investigators to do the analysis and draw the conclusions. This may affect the quality of the gathered information of the incident and impair the engagement of local management and controllers.
The vast majority of the reported occurrences are mainly used for giving headquarters a rough idea of current problem areas, where actions should be taken. They are only processed locally to a slight degree, i.e. local learning is limited.

2. Only the “tip of the iceberg” of the information is used for improving flight safety. When the evaluation of current methods and procedures is based on single, rather serious cases (AIRPROX-incidents), there will often be a tendency to suggest crude corrective actions, based on ‘‘snapshot’’ information. This might create a range of new problems because the information platform is too small, or, in other words, the suggested corrective action does not take into account the complexity of the problem and may introduce new complexity (and new risks).

A general problem with reporting systems, in order to learn about the risks in a system, is the degree of the operators awareness of risk. With a low degree of risk awareness only rather salient occurrences will be reported, i.e. occurrences concerning near misses or AIRPROX. With a higher degree of risk awareness operators may start to report occurrences where ‘‘nothing actually happened but there was a risk that something could have happened”. ‘‘Nothing’’ in this context means traffic situations without ‘‘last second’’ error recovery but with the potential, according to the controller’s judgement, to give rise to dangerous situations.

It was our belief, to be assessed in the study, that with a higher degree of risk awareness among the controllers, more perceived risks would be documented, and thus made accessible for safety improvements.

There is a tradition amongst controllers (probably not only in Sweden) of discussing the events of the day (mainly traffic resolutions that did not work out satisfactorily) in the coffee room. However, the information acquired from these cases goes no further. If these discussions were to take place in a more organised manner they might better contribute to improving team safety awareness concerning risks.

A management decision at the ATCC Malmoe was made to conduct a trial using a local reporting system, called ‘‘learning occurrences’’, with the following aims:
• To make better use of the learning value from non-AIRPROX cases.
• To achieve a deeper and more systematic engagement from the controllers in the flight safety improvement process.

The study questions were formulated as follows:

• What can be learned about how to market a reporting system for the controllers, and about how to train them?
• Is it possible to identify certain risk patterns from the reports?
• What can be learned about recovery from process disturbances?
• Is expert support needed, and if yes, when and for what purpose?
• Will the reporting system produce suggestions for concrete flight safety improvements?

Before we started the trial all controllers (200) were trained for a day in systems thinking. Amongst other areas we used examples from health care and sea transport, and avoided examples from air traffic control because we have experienced that the controllers would delve into technical details in such cases with a degree of delight, thus missing the overall message.

The controllers were asked to report

- Late conflict detections
- Forgotten, missed or misunderstood co-ordination
- “Interesting” traffic situations.

The reports would be analysed at the authorisation group meetings (only controllers present). The local flight safety group (with controllers only) would bimonthly survey all the reports,

for “lessons learned”, and a human factor/safety expert (corresponding author) would attend and facilitate these meetings.

During the trial period of six months 44 reports were filed, concerning safety occurrences that otherwise would not have been reported. The controllers themselves identified system weaknesses (latent failures and lack of safety barriers) in 40 of these cases. For the remaining three cases the safety expert interviewed the reporting controller for completion.
It was not unusual that the reporting controller spontaneously blamed him/herself: “I should have looked more carefully…”or “I missed looking out for a conflict when I changed the clearance.” In the group discussions on such cases we tried to market a systems view instead of individual blame.

A success criterion was if the trial resulted in concrete safety improving actions.
Which it did.

One identified item concerned the computer-generated names of waypoints (the waypoints are defined by latitude and longitude, and fed into the aircraft flight management system. The autopilot will automatically fly the aircraft from one waypoint to the next, and to the next etc.) The problem was that the computer-generated four to five letter names of waypoints could create confusion on the flight deck, making the pilot choose the wrong waypoint, as for example the similarity of waypoint names such as RISMA and MISMA.

A second problem concerned the controller’s lack of knowledge on how a flight management system (FMS) “thinks”. When an aircraft is closing in at the airport of destination the FMS computes the proper time for the aircraft to start to descend from level flight. It uses input variables such as aircraft speed, aircraft weight, current wind conditions, remaining miles to touch down and even passenger comfort. The FMS wants to do this as economically (fuel wise) as possible, which means cutting the engines to idle, i.e. the aircraft will glide.
A standard clearance from air traffic control is “descend when ready”, i.e. the controller leaves the time for starting the descent to the pilot, which leaves the decision to the FMS. However, the controller does not know all the computational parameters used by the FMS. Thus the aircraft might start to descend earlier or later than the controller had anticipated, creating unexpected conflicts with lower traffic.

It was decided that the controllers should receive training on the FMS. Some pilots provided lessons on this, which was much appreciated by the controllers.

A third identified risk concerned the relief procedures for controllers. A number of reports pointed at the relief procedures being too fast, not enabling the new controller to acquire adequate situational awareness of the traffic when the responsibility was handed over. New procedures were implemented.

A fourth risk was about acquiring as comprehensive information as possible on safety occurrences. Traditionally controllers often blamed the pilots for mistakes such as "unexpected aircraft behaviour".
There was no tradition for the controllers to talk to the aircraft crew, - such contacts should, according to procedures, go via headquarters and the regulator, i.e. the controllers should ask headquarters to ask the crew something and would eventually, after some months, get an answer, meaning that this procedure was cumbersome and of limited value for getting safety feed back from the flight deck.
During the trial period the controllers began to communicate directly with the aircraft crew, so as to get the narrative from "the other side", and they realised that they in a number of cases actually themselves was the cause of flight deck confusion and subsequent "unexpected aircraft behaviour". One example was the best intention of the controllers to give as direct a route as possible, thus saving both flight time and fuel. As long as the new direct route was to a waypoint further along the already programmed route it was easy for the pilots to reprogram the FMS. However, sometimes the controller's offer for a direct route involved using waypoints not contained in the original flight plan. The pilot then had to search for this waypoint in the FMS menu, and maybe failed to find it until page seven in the menu. This could prove to be quite cumbersome, and if this reprogramming coincided with other pending flight deck matters the result could be pilot mental overload, and incorrect programming of the FMS, and thus "unexpected aircraft behaviour". The controllers were unaware of this until they received training on the FMS.

The conclusion from this user-centred approach was very positive. The controllers were very able to do the analysis and suggest improvements, and they felt they were the "owners" of the problem of safety improvements.

Paper IV. System weaknesses in the process of treating patients with cytotoxic drugs.
The setting for this study was the department of oncology, and the hospital pharmacy, at the university hospital in Lund, Sweden.
From lessons learned from paper II we established from the very beginning a reference group consisting of a doctor and a nurse, and this was of great help when conducting the risk analysis in this setting.

The analyst team consisted of a pharmacist, the corresponding author and a nuclear plant control room engineer.

Why a control room engineer? We believed that an interdisciplinary approach might be fruitful. Furthermore, the corresponding author and the engineer had previously done a proactive safety analysis on one of the start up processes on a Swedish nuclear reactor, after the plant had been shut down for yearly maintenance. So we reversed the roles, changed domains so to speak.

The aim was to use the DEB analysis on the process of treating patients with cytotoxic drugs. Some of the identified latent failures were:

The procedures for updating the manual with chemotherapy regimes are unsafe.
There was no guarantee that a certain hard copy of the manual was properly updated. Putting the manual on the Internet solved this (though it introduced a new risk, - improper updating on the Internet).

The procedures for cooperation between the pharmacy and the department of oncology are implicit and not clear.
One risk concerned illegible prescriptions. Procedures state that the pharmacist must verify such a prescription. However, according to interviewed pharmacists as a rule it was not possible to contact the responsible doctor. And if they did they quite often the response he/she gave was impertinent.
This induced certain reluctance on the part of the pharmacists to contact doctors, and as a result they started making guesses about the contents of the prescription.
This problem has been remedied by the computerization of this procedure.

Another identified risk is that the pharmacy, if time so permits, makes a check of the doctor's calculation of dosage of a cytotoxic drug, based on the patient's body area. The problem lies in that the doctors being convinced that this procedure was mandatory for the pharmacy.

A couple of identified latent failures were the manual transfer of information from the cytotoxic manual to the treatment sheet. Human operators are not particularly good at this and often make transfer mistakes. Now electronic transfer from the Internet deals with this risk.

A latent failure concerned the infusion pumps for administering the cytotoxic drugs. One ward unit had one brand of pumps only, another unit another brand. During workdays this was not a problem, but during weekends and holidays the two units would share staff, meaning that staff accustomed to one brand of pump had to operate a pump unknown to them.

The results of the DEB analysis were presented to management and all staff at a meeting. We were quite anxious before the meeting, but the latent failures were accepted as relevant, and so were our suggestions for corrective actions. Quite a few of the recommendations were later implemented.
We believe that the use of a reference group was important for giving us the credibility we strove after. We have experienced that what professionals really detest is outsiders claiming that they understand the processes, but showing that they do not. Another experience is the opposite, - professionals really respect outsiders who earnestly and humbly try to understand what they are doing.

Discussion

In this thesis four different approaches were tried for safety related feedback and the pros and cons for each will be discussed.

In this section I will first discuss our results for each research question in relation to current research.
Then I will introduce a new paradigm, a postmodern way of looking at complex systems, *complexity theory*
After this introduction I will reflect on the results in relation to complexity theory, which will pave the road for posing some interesting questions for future research.

Addressing the research questions

1. *Is it possible to use Reasons' notion of a systems view in health care, and thus identify latent failures and insufficient safety barriers?*

The answer is definitely yes. Some five years after the publication of paper I the legislation was changed, amongst other measures by abolishing the Disciplinary Board in its current shape (though of course not just because of this study).

According to my literature search very few health care organisations use MTO analysis. However, a wide spread method for retrospective analysis of incidents is the Root Cause Analysis (RCA). Though having a modern system thinking it strangely enough does not use the Reason terms of active failures and latent conditions (as the MTO analysis does). This might be one reason for the difficulties of the RCA analysts to formulate corrective actions.
Another reason for this could be that the analysts have poor knowledge on the components of a quality (safety) management system (e.g.like ISO 9000).
A suggestion is that Reason's concept be incorporated in the RCA.
Another suggestion is that analysts be trained in what a quality management system looks like, how it works, and what the interdependencies look like.
Without this fundamental knowledge I can understand that analysts have difficulties formulating suggestions for corrective action.

Very few articles (two) describe the experience of RCA. A critical commentary in BMJ points at a lack of consistency when using the RCA, many RCAs producing no usable results at all[41].

2. *To design a method for proactive risk analysis for systems such as health care and air traffic control.*

A proactive method, the DEB-analysis, was designed and inspired by the experience from the health care accident analyses (paper I). As previously mentioned none of the existing models fit our purpose. The Hazop method was designed for finding risks when monitoring and controlling the flow of energy and matter in process plants.

A wide spread method in health care is the FMEA method, also originally designed for technical systems. What we especially disliked with this method was its use of a hazard-scoring matrix (see further description of the method under "Theoretical considerations"). In this matrix a score is given for "probability" that a certain failure will take place, from "frequently" to "remote"(of which the analyst can know very little).

In the matrix the analyst will then have to score "severity of effect" of the identified failure. As we have pointed out earlier, the consequences of a failure is impossible to predict in a complex system, - the effect can be anything from fatal to no effect at all, depending upon a lot of interactions in the system (see further on *complexity theory* in this section).

Finally, the scores for effect, detecability and probability will be multiplied to create "a hazard score".

In my opinion this is more than questionable. If one multiplies a score for frequency (which is very uncertain) with a score for effect (where the prediction may be everything from fatal to none for a certain failure mode), and a score for guessing on how easy a failure can be detected, a result of, say "16", will have no meaning at all. One uncertainty multiplied with two other uncertainties is indeed very uncertain.

In this respect it is not astonishing that two different FMEA teams, analysing the same process, end up with quite different results, as described in the article by Shebl and Franklin: *Is failure mode and effect analysis reliable?* (see further under "Theoretical considerations").

3. *To try out this method for identifying latent failures (and insufficient safety barriers) without waiting for an accident to disclose these system weaknesses.*

We were conducting the maiden voyage for the DEB analysis in a totally new setting, namely air traffic control.
The ability of the method to identify relevant latent failures was measured by comparing the results from the DEB analysis with actually disclosed latent failures from the last years AIRPROX incidents. The "hit rate" was 93 %.

It was cumbersome and hard work trying to understand the mysteries of air traffic control (but the controllers were good teachers!). A positive side effect was to experience that a method inspired by and tuned for health care actually worked well in a totally different domain.

As this was the maiden voyage for the DEB analysis there was of course a number of lessons learned when applying the method. The most important was that a formal reference group of staff should be appointed from the very onset, helping the analyst with the task analysis, joining in brainstorm sessions about possible disturbances and their effects, and facilitating suggestions for the engineering of safety barriers.

We even experienced that proper "marketing" of the analysis was important. There was a tendency for controllers to defend their system. The same tendency was noticed for doctors in paper IV (not the team doctors, but other doctors who were interviewed).

4. *Was it possible to increase safety consciousness for the air traffic controllers by giving them responsibility for collecting and analysing "safety occurrences", i.e. increased user participation at the expense of expert dependency?*

All the controllers were trained according to a defined curriculum of one day, teaching them systems view and the basics of doing a MTO analysis and a DEB analysis. The reports they analysed were a mixture of occurred “near misses” (which calls for a MTO like approach), and perceived risks that are closer to a DEB approach.

During training we used examples from health care and sea transportation, and avoided examples from air traffic control because we have experienced that the controllers with delight would delve into technical details in such cases, thus missing the overall message.

They received the ownership of the reporting an analysing. During the trial period of six months they reported 45 “safety occurrences” which would not otherwise have been reported, and this resulted in six concrete safety improvement actions, such as giving the controllers education on the aircraft flight management system, and the renaming of navigation waypoints which could not be confused.

Thus the answer to this research question is that it is feasible to increase user participation at the expense of experts when it comes to collect and analyse safety critical information. The study also showed that training of users made them to report more safety critical information than was mandatory. Unfortunately these effects seemed to be rather temporary. The reporting and analysing faded out quickly after the trial period. One reason for this might be the change of management at that time, the new management being less interested in this kind of safety initiative.

5. To perform a DEB analysis with a well defined and formalised user participation.

Finally we could return to health care, oncology and pharmacy. It was of great help to the analysts to have a reference group from the very outset, consisting of staff from the department of oncology, and it also increased our credibility vis-à-vis the management and team of doctors. After all, it was people from their own ranks who had contributed to the result of the analysis.

In the aftermath of the analysis we have noted that a fair amount of our suggestions had been implemented. Actually we wanted to document this follow-up in a scientific article but lacked support, time and finances for this. This we considered to be a pity since the literature on good follow up studies is scarce.

Relating the thesis to complexity theory

In all the papers we have used terms like "complex systems", or "complex socio-technical systems". These terms have in the safety management literature been rather crudely defined (or not defined at all) as "a system containing a lot of technical equipment", alternatively "a system with a lot of people and technical equipment". This is not very satisfying and can easily create confusion.

To take an example: A modern jet aircraft is a technical system. When a handle is manipulated, or a button pressed, it is very predictable what will happen.
But when you place two pilots at the flight deck, is it still only a technical system, or a complex system, or a complex socio-technical system? To me the distinction between a complex system and a complex socio-technical system seem fuzzy.

Introduction to complexity theory. Paradigms.

A clarification may best be endeavoured by focusing on complexity theory.
I will begin with Thomas Kuhn, one of the most influential postmodern science theorists. He claimed that the scientific norm systems change over time. These norm systems he called *paradigms*. The paradigms, he said, govern which questions are considered relevant, which methods should be used, and what the scientific argumentation will look like.[42]

One such a paradigm is complexity science.
The main part of the work with the papers for this thesis was accomplished in the late nineties and beginning of the twenties. Complexity science as a paradigm was lifting off beginning of the twenties and thus not integrated in the papers. On the other hand, as mentioned previously, we intuitively incorporated complexity in our thinking, feeling that linear models with straightforward cause –effect relationships did not fit our research areas.

When discussing complexity we can go back a long time in history, to the Aristotelian holistic statement that "The whole is more than the sum of its parts"[5].
However, Aristotelian teleology[6] was eliminated during the later development of Western sciences, during the Scientific Revolution in the 16th and 17th centuries. It was replaced by positivism[7] and reductionism.

[5] Aristotle, Greek philosopher, 384 BC – 322 BC.

In Descartes[8] second maxim in "*Discours de la méthode pour bien conduire sa raison et chercher la vérité dans les sciences* "[9] one should "brake down every problem into as many separate simple elements as might be possible", meaning to reduce complex phenomena into elementary parts. This was reductionism (or "Cartesian" reductionism).
This worked remarkably well as physics was concerned (Newtonian mechanics[10]), but failed to explain why living organisms did not degrade according to the second law of thermodynamics, towards destruction of existing order and ultimate decay.

During the first decades of the 20th century increasing doubts were expressed concerning this "paradigm" of classical sciences, i.e. the reductionist way of thinking and analysing. It failed to explain complex phenomena in terms of isolable elements, such as the behaviour of biological systems, and also of social systems. This led v. Bertalanffy, a theoretical biologist, to propose a General System Theory in 1930[43]:

> There exist models, principles and laws that apply to generalized systems or their subclasses irrespective of their particular kind, the nature of the component elements, and the relations or "forces" between them. We postulate a new discipline called General System Theory. General System Theory is a logico- mathematical field whose task is the formulation and derivation of those general principles that are applicable to "systems" in general. In this way, exact formulations of terms such as wholeness and sum, differentiation, progressive mechanization, centralization, hierarchical order, finality and equifinality, etc., become possible, terms which occur in all sciences dealing with "systems" and imply their logical homology.[44]

With a starting point in v. Bertalanffy's General Systems Theory, ideas progressed towards the paradigm of complexity theory and complex adaptive systems (CAS), as expressed by Cillier in his volume *Complexity and postmodernism, understanding complex systems* [45].

Basics of complex systems

---

[6] A **teleology** is any philosophical account which holds that final causes exist in nature, meaning that design and purpose analogous to that found in human actions are inherent also in the rest of nature. The word comes from the Greek *τέλος* - *telos*, root:*τελε-*, "end, purpose."
[7] Positivism: the paradigm that there is one and only one truth concerning a phenomenon. This truth could be found by using Cartesian reductionist methods.

[8] 1596-1650

[9] 1637
[10] Sir Isaac Newton, 1642-1727. Main publication: *Philosophiæ Naturalis Principia Mathematica*

The basics of complex systems are summarised in this table, as well as the interpretations in relation to the thesis:

Characteristics of complex systems	Implications/interpretations in relation to thesis
Complex systems are open systems, continually exchanging information with the environment. The internal structure of the system can adapt dynamically to changes in the environment.	Both health care and air traffic control are open systems. They have to adapt to budget cuts, increases in number of patients (or decreases in number of flights, as during the eruption of the Eyafjällajökull).
Complex systems show self-organisation. This is not merely the result of feedback loops or regulation that can be described linearly. It involves higher-order non-linear processes.	The studied organisations organise itself due to external influences. New focus groups and new procedures emerge in an unforeseen way.
Self-organisation is an emergent property of the system.	See above.
Self-organizing systems increase in complexity. Since they have to learn from experience (they have a "history") they "remember" previously encountered situations and compare them with new ones. This implies a local reversal of entropy.	Different departments at a hospital, or different air traffic control centres, have their unique history. A sensitive visitor can feel differences in "climate".
The information (memory) in a complex system is weighted according to how frequently a certain cluster of information is present.	When information clusters include safety occurrences this information will be weighted high, especially if it is repeated (as in paper III).
The elements in a complex system interact dynamically. Individuals are engaged in a constant exchange of information.	Meaning that you cannot know the impact of external information fed into the system
Human individuals interact with many others in a vast array of different capacities. These interactions are non-linear.	Tell a complex system what to do, - you cannot really be sure what comes out of it.
The interactions have a fairly short range. The elements in a complex network interact primarily with those around them.	The individual operator talks to his/hers pals about the new external information. What comes out of it you cannot know for sure.
There are loops in the interconnections. Information is proliferated throughout the system and is continually transformed, by other bits of information. Thus it is impossible to stipulate a "true" interpretation for any piece	This means that central databases containing "all safety occurrences", and all the answers, have a very limited value when it comes to influence a complex system. Information is local, coupled to a

of information. Information can only be interpreted locally. Information is contingent, pertaining to a certain context and a certain time frame.	certain time frame and a certain context. Which central databases do not take into account.
Complex systems have histories. This history is not an objectively given state. It is a collection of traces of information distributed over the system, and it is always open to multiple interpretations.[11]	You can never be sure about the history of a complex system. You may think that learning from the last ten safety occurrences should be vivid in the complex system's history, but you cannot be sure.
Individual elements are ignorant of the behaviour of the whole system in which they are embedded. Single elements cannot contain the complexity of the whole system and can therefore neither control nor comprehend it fully. No complete picture of the system's present state is available to anyone.	This applies to managers as well. If they claim that they are "in control" of the system they are accordingly wrong.

Table 1. *The characteristics of a complex system, according to Cillier, are summarised in the left column of the table. In the right column the implications for this thesis is subjectively interpreted by the author.*

After this brief we return to our "research settings", and attempt to argue that the studied systems indeed are complex systems, in its true sense, i.e. behaving according to complexity theory.

The behaviour of a complex system is unpredictable. Its units defines its own goals and act accordingly. A complex system defies central control. It acts according to what its agents (doctors, nurses, air traffic controllers) find important for obtaining "good".

What does this paradigm imply for risk management in complex systems such as health care and air traffic control? A complex system way of thinking is opposed to the Newtonian way of looking at things. The implication of this is that it is not possible to get a meaning of the whole by examining its parts. As an example, it is not possible to understand an accident by analysing only the behaviour of the "agents" who committed an error. To believe that is to return to determinism. Instead one should try to understand how the system had adapted to the surrounding reality. What were the goals of the unit? Which were the emergent properties? What were the inputs from the surroundings to which the system adapted?

[11] This applies to postmodern society. Postmodernism rejects an interpretation of history that elevates it to a master key for unlocking the true meaning of present conditions. There is no true meaning.

The concept of risk management in complex systems could then be formulated as a way to influence the adaptive behaviour, and the emergent properties, of the system towards increased awareness of risks, i.e. that the system includes increase of safety as part of its goals.

One emergent property could be ” increased awareness on safety matters”. The more safety occurrences are repeated it becomes a stronger part of the system’s memory. This will influence the adaptation mechanisms of its agents, the individual agent becoming more alert to risks when carrying out his/her tasks. An emergent property may be that the documentation and discussion of these risks add further to the memory of the system. That is, not only *de facto* occurrences will be documented but even “could have been” occurrences.

One way of illustrating the self-organising behaviour of a complex system is the adaptation due to environmental influences, as depicted in Rasmussen’s “design envelope”[46]. According to this the system fluctuates around some kind of equilibrium, trying to obtain a balance between the exploitation of the work force, efficiency and safety.

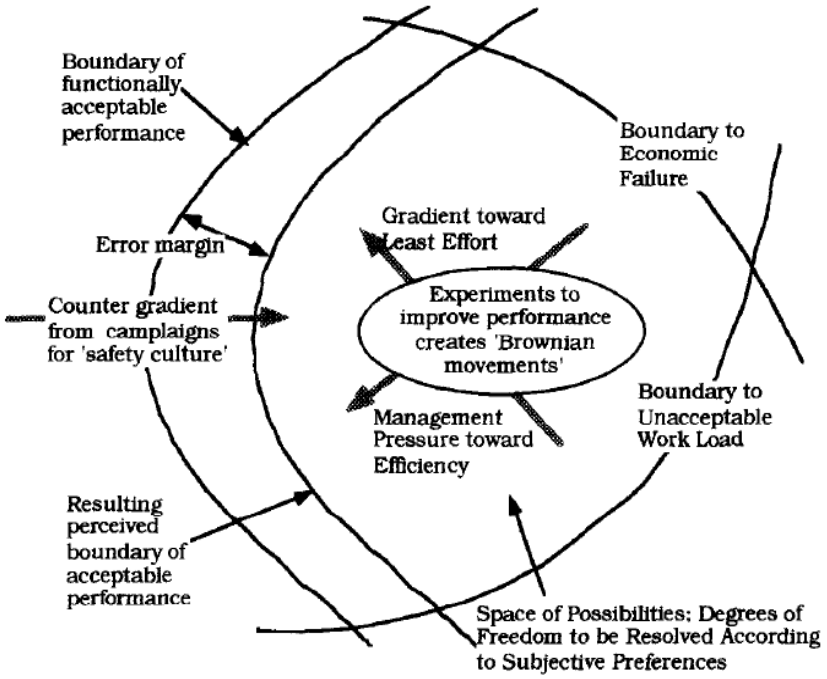

Figure 4. Rasmussens design envelope. Rasmussens figure text: "Under the pressure of strong gradients behaviour will very likely migrate towards the boundary of acceptable performance" [47].

A strong drive from the environment (owners/stakeholders) is to maximize profits. This can be obtained by making the workers work harder. A counterforce against misuse of the working force is the working environmental legislation. Profits may also, at least in the short term, be increased by adopting less safe ways of doing things. A counterforce against this is a declining safety record. Where a complex system actually ends up in this "envelope" is impossible to foresee. The interactions and co-dependencies in the system do not follow any regularity/linearity. If we should be able to anticipate this we would have to know exactly how each component would behave. Then we could describe it in an equation. But we cannot.

With this account of complex system characteristics we do not find the claim that the studied systems indeed are complex systems, particularly controversial. They are definitely open systems, acting to requirements and pressures from the surroundings, concerning amongst other factors a good safety record and efficiency.
They adapt to these using different strategies, based on their "memory", and will internally organise to meet these requirements. They will constitute working groups for dealing with patient (air traffic control) safety.

Complexity theory tells us that a top-down approach with an external agent ordering the system to act in a certain way will not work. If we do this anyway the self-organisation and adaptation of the system will make it impossible to foresee which emergent properties will come out of it. Instead we should try to influence the system in such a way that a large part of its goals will emerge as increased focus on safety improvement.
Can we deduce from complexity theory some principles for how a complex system should be fed information? According to Cilliers:

> Self-organising systems increase in complexity. Since they have to "learn" from experience, they have to "remember" previously encountered situations and compare them with new ones. If more "previous" information can be stored, the system will be able to make better comparisons.

> [...] Self-organisation is impossible without some form of memory. Without memory the system can do no better than merely mirror the environment…Memory, on the other hand, is impossible without some form of selective forgetting…Information that is not used simply fades away…The more something is used the stronger its "representation" in memory will be[48].

Further:

> If a certain cluster [of information] is present regularly, the system will acquire a stable set of weights that "represent" that cluster, i.e. a certain pattern of activity will be caused in the system each time this cluster is present.[49]

What does this tell us for feeding information to a complex system?
First, that it should be done on a fairly regular basis. One quick shot of information may have a very limited time span in the memory of the organisation, and may quickly fade away. Some traces of safety critical information may exist for a while, but we have no way of anticipating which properties will emerge. And we do have an idea of a desirable emergent property, namely increased safety consciousness.

Secondly (and complexity theory does not explicitly say this) the more a certain cluster of information is perceived as the "property" of the system the heavier the weight of this information when it comes to shape the goals of the system, i.e. the notion of "goodness".

How to influence complex systems, related to this study
On this we can think of a model how to influence the system, and compare it with the different approaches for learning used in the papers I-IV.

For the MTO-analysis (paper I) an external agent is feeding the system information on what the risks in the system actually are. A problem with this is that the external agent is "telling" the system what the risks are, as if it is a "true" (positivistic) narrative of risks. But it is not. The external agent has made a lot of (subjective) choices for defining this "truth" but there are a lot of other truths. So, the MTO analysis is feeding the system with information, which can be misunderstood by the system as the one and only "truth", and thereby restricting fruitful feedback loops. No repetition is involved, thus the memory trace of this information bears little weight and may soon be forgotten.

On the other hand, if the external agent is a regulatory body it can force the system to deal with this information, for instance requiring that corrective actions be taken inside a certain time frame, and inspecting what actually has been done.

Respond to criticism of MTO analysis

Paper I is the only paper dealing with accident analysis. Dekker, Cilliers and Hofmeyr has in a paper criticised traditional accident analysis[50]. Their criticism is that the analyses are done in a positivist way, assuming that there is a "truth" about the accident, and that the analyst can disclose this truth if only the proper methods are used. Some of their conclusions are that there is no "truth" to disclose, that the system has changed from the time of the accident to for instance the time where the accident report is published, and that there is no linearity between component behaviour and system-level outcome.

In the light of this criticism we would like to defend the way we have used the MTO analysis. First, we never tried to tell "the true story" of an accident. Instead we attempted to tell a story about latent failures in the system, and how these latent failures may have, or maybe not, played a role in the accident. One of our main points, when demonstrating the results of the analysis for department management, was to argue for the risks they had in their system, disclosed by the analysis. Management had a general tendency to discard identified risks as not being relevant, but we could easily show that the risks were indeed relevant. In fact they already had contributed to an accident (quite a strong argument), and if not dealt with they would sooner or later contribute to another. Thus the MTO flow chart was a powerful pedagogical tool.

In our use of the MTO analysis we distanced ourselves as much as possible from root-cause analysis when formulating the latent failures (we were inspired by the vocabulary used in the ISO 9000 standard for quality systems. The corresponding author is a trained ISO 9000 auditor).

On complexity and safety barriers

The notion of safety barriers seems not to be contained in a complex system theory. The thinking is linear: If operator A does this (wrong) action we engineer a constraint which either makes it impossible for him/her to perform this action, or the constraint will swallow the wrong action before it hits the system. How then can a linear notion fit into a non-linear

system? We think the answer is that in the processes of a complex system there might be pockets of complicatedness[12]. We can isolate these pockets and thus apply the safety barrier notion[51].

To give an example: Medication to patients at a ward unit will partly be complicated, partly complex. But if we isolate a tiny part of this process such as one nurse preparing the administration of drugs by collecting the drugs from the drug cabinet and placing them in the appropriate patient cup, for later dispensing, we could say that this process was complicated, not complex. There is no interrelatedness in the exchange of information.
We can then discuss barriers such as the nurse double-checking after having dispensed the drugs in the patient cups. Or we can discuss the use of bar codes for transforming an administrative barrier to a (almost) technical one.

On the other hand, this is not the whole story. Emergent properties in this ward unit have adapted to various inputs from the environment. These inputs could be a shortage of staff creating a degree of stress for the nurse. Or they could be a lack of incident feedback loops, making the dispensing of drugs a somewhat disorganised process. Thus the borderline between complicated parts of the system, and complexity, will be fuzzy and floating. The meaning with this argument is that even if we adapt the postmodern notion of complexity we should not become nihilistic. We can identify these "pockets of complicatedness" and use linear thinking. Thus bar codes, standardization of treatment and similar barriers are feasible even in complex systems.

Management and adaptation

In paper II, an external agent is again defining the risks and giving this as input to the system. The pedagogical argument with management is much weaker than in paper I. When we account for identified latent failures the management might say: "No, I do not believe this, it is not really a risk". And we cannot argue, "Look, it has already created an accident". However, management engagement can reinforce the impact of the information the same way as suggested above for paper I by requiring corrective actions. The system will adapt and self-organise according to these requirements.

[12] A modern aircraft is a complicated system. If it is manipulated in a certain way the effect is foreseeable. But when we put pilots in this system it is longer foreseeable, - it gets complex.

The "best way" to influence a complex system…

Of the studied approaches paper III seems to offer the best way of influencing a complex system. The feedback loops are clearly defined and will repeatedly feed the system with information on risks, and the information will be "owned" by the operators, creating a rich background of information for adaptation and self organising.

However, this approach was not self-sustaining, on the contrary. It needed constant attention and coaching from management, the flight safety group and the corresponding author. After some months after the trial period was finished I conducted a follow – up study. The organisation had adapted in a non-desirable way. Interviewed air traffic controllers responded that they did not report new safety occurrences "because this problem has already been reported previously. No need to do it again.

The operative management changed and was not interested in this safety approach. The flight safety group was disinterested in further reporting and analysing and had defined new goals for their activities.

So after a year the entire concept had been abandoned.

For paper IV the same comments can be made as for paper II but also show an interesting difference. The management at the department of oncology took the DEB analysis very seriously. It organised itself in several working groups and the result was that a fair amount of the disclosed risks and suggestions were taken care of.

Gap between influence on complex systems and sustainability

From these experiences a new research question gradually emerged.

The problematisation is the following: An operator owned approach for feeding a complex system with continuous input appeared to be a good idea. The memory of the system would continuously be fed with information on safety. This memory would become progressively richer in details over time, making the system increasingly better in making comparisons. The system might adapt and self organise according to this "safety information", which would create a strong representation in the memory of the system.

However, even if the approach used in paper III fulfilled most criteria for influencing a complex system it was not very stable over time. Thus we seem to have a gap between influencing a complex system safety wise and a good, stable method for which to do it. To identify this/these method (s) can be a new research area.

Conclusion

Concerning the overall research objective, to test different ways of learning and influencing a complex system, we conclude that the user owned method (paper III) probably is the best of the tested approaches. It feeds the system with safety critical information on a daily basis. The system will have to adapt to this information, which probably will have a strong representation in the system's memory , and due to this continuous input the system's knowledge will become richer. However, this approach was far from self-sustaining.
Thus there seems to be a gap between influencing a complex system towards self-organising, and robust methods for doing this. Developing this concept could be an interesting topic for future research.

Future research

A hybrid method between retrospective and proactive error management is the "Tripod-Delta", originally designed by Shell for oil exploration and production operations. It is described by Reason in detail in [52] and in[53]. Tripod Delta defines 11 general failure types, which very much overlap with requirements to a quality management system as stated in the ISO 9000 standard.
Some of these are:

- Hardware
- Design
- Maintenance management
- Procedures
- Incompatible goals

For each general failure type a set of some twenty indicators has been worked out by the work force on the floor, which is one of the appealing factors of Tripod, i.e. it is "owned" and managed by the "floor workers", who are closest to the risks during operations.

As soon as a risk or other shortcomings in the processes are noted, they are fed into the Tripod-computer. At regular intervals computer generated score tables for the different general failure types are presented to the workers and line management, in order to help them prioritise the safety activities for the next couple of months.

For influencing a complex system to improve safety we find this method interesting (and have started a research project for testing within health care). Referring to the discussion above how to influence complex systems the Tripod-Delta will constantly update the memory of the system. Regularly the Tripod computer program will feed safety related problems into the system, to which the system will have to cope (adapt) accordingly. The Tripod provides quite a robust first order feed back loop. On a regular base the Tripod software will provide information on which general failure types are to be worked on. If this is not accomplished the Tripod program will show this during the next run.

Since the literature on RCA points at a non-consistent way of using the method (mainly US and UK), frequently producing useless results, maybe the MTO analysis could be a fruitful alternative. Thus a research area could be to try the MTO method in other European countries.

FMEA is widespread in the US and UK but apparently can produce very different results for the same process. Since the FMEA relies on a very dubious “hazard score”, as we have discussed above, it could be of interest to apply the DEB in an environment accustomed to FMEA, and compare the results from FMEA and DEB for the same process.

References

[1] Bogner MS (ed.). *Human error in medicine*. Lawrence Erlbaum Associates, New Jersey. 1994.

[2] Bosk CL. *Forgive and Remember*. Chicago: University of Chicago Press, 1979

[3] Reason J. *Human Error*. Cambridge University Press, 1990.

[4] Vaughan D. The *Challenger Launch Decision*. The University of Chicago Press, Chicago, 1996.

[6] Vaughan, p. 394.

[6] Dekker S. *The Field Guide to Understanding Human Error*. Ashgate, Aldershot, England, 2006.

[7] Dekker, p. 15.

[8] Perrow C. *Normal accidents, Living with high-risk technologies*. Princeton University Press, Princeton, 1999.

[9] Perrow, p. 4.

[10] Sagan SD. *The limits of safety. Organizations, accidents and nuclear weapons*. Princeton University Press, Princeton, New Jersey, 1993.

[11] Sagan, p. 257.

[12] Koornneef F. *Organised learning from small-scale incidents*. Thesis. Delft University Press, Delft, 2000.

[13] Reason J. *Managing the risks of Organizational Accidents*. Ashgate, Aldershot, UK, 1997.

[14] Ek Å. *Safety culture in sea and aviation transport*. Thesis. Department of design sciences, Lund University, Sweden, 2005.

[15] Lindberg A-K, Hansson SO, Rollenhagen C. Learning from accidents – What more do we need to know? Safety Science, 48:714-721, 2010.

[16] Swedish National Board of Health and Welfare, Act 2005:28, http://www.socialstyrelsen.se/lexmaria

[17] Swedish National Board of Health and Welfare, Act 2005:12, http://www.socialstyrelsen.se/sosfs/2005-12

[18] ISO 9000 International standards for quality management, 1996. Stockholm, SIS förlag.

[19] Wiegmann DA, Shappell SA. *A human error approach to aviation accident analysis*. Ashgate, Aldershot, England, 2003.

[20] Koornneef F. *Organised learning from small-scale incidents*. Thesis. Delft University Press, Delft, 2000.

[21] http://www.google.se/images?hl=sv&biw=1680&bih=955&q=swiss+cheese+model&um=1&ie=UTF-8&source=univ&sa=X&ei=aXR4Tby3DYPEsgaC7bGxBg&ved=0CCsQsAQ, accessed 2011-03-10

[22] Rasmussen J, Svedung I. *Proactive risk management in a dynamic society*. Swedish Rescue Services Agency, Karlstad, Sweden, 2000.

[23] Ternov S. The human side of medical mistakes. In Spath P (ed.). *Error Reduction in Health Care*. New York, Jossey-Bass, 2000.

[24] Bosk CL. *Forgive and Remember*. Chicago: University of Chicago Press, 1979.

[25] Hollnagel E. *Barriers and accident prevention*. Ashgate, Aldershot, England, 2004.

[26] Hollnagel, p. 68.

[27] Percarbio KB, Watts BV, Weeks WB. The effectiveness of root cause analysis: What does the literature tell us? Jt Comm J Qual Patient Saf. 34(7), 391-398, 2008.

[28] Vincent C, Taylor-Adams S. *Framework for analysing risk and safety in clinical medicin*e. BMJ 316(7138):1154-1157, 1998.

[29] Vincent C, Taylor-Adams S, Chapman EJ, Hewett D, Prior S, Strange P, Tizzard A. *How to investigate and analyse clinical incidents: Clinical risk unit and association of litigation and risk management protocol*. BMJ, 320:777, 2000.

[30] Wu AW, Lipshutz AKM, Pronovost PJ. *Effectiveness and Efficiency of root cuase analysis in medicine*. JAMA, 299:6, 2008.

[31] Spath PL. *Using failure mode and effects analysis to improve patient safety*. AORN J, 78(1):16-37, 2003.

[32] Robinson DL, Heigham L, Clark J. *Using failure Mode and Effect Analysis for safe administration of chemotherapy to hospitalized children with cancer*. Jt Comm J Qual Patient Saf, 2006, 32(3):161-166.

[33] Shebl NA, Franklin BD, Barber N. *Is failure mode and effect analysis reliable?* J Pat Saf, 5(2):86-94, 2009.

[34] Reason J. *Human Error*. Cambridge University Press, 1990.

[35] *ISO 9000 International standards for quality management*, 1996. Stockholm, SIS förlag.

[36] .INPO (Institute of Nuclear Power Operations): *Human PerformanceEnhancement System, program description*. INPO document INPO 90-005, Atlanta, 1990.

[37] Rollenhagen C. *MTO – en introduktion*. Utbildningshuset Studentlitteratur, Lund, 1995. In Swedish.

[38] Taylor JR. *A background to risk analysis*. Electronics department, Risö National Laboratory, Denmark, 1979.

[39] International Electric Commission (IEC). *Analysis techniques for system reliability,- procedure for failure mode and effect analysis.* IEC, Genève, 1985.

[40] Chemical Industry and Safety Council. *A guide to hazard and operability studies*. Chemical Industries Association, London, 1981.

[41] Wu AW, Lipshutz AKM, Pronovost PJ. *Effectiveness and Efficiency of root cuase analysis in medicine*. JAMA, 299:6, 2008.

[42] Kuhn, T. *The Structure of Scientific Revolutions*, University of Chicago Press, Chicago, 1970.

[43] Bertalanffy L von. *General systems theory*. George Braziller, New York, 1968.

[44] Bertalanffy, p. 32.

[45] Cilliers P. *Complexity and postmodernism, understanding complex systems*. Routledge, New York, 2005.

[46] Rasmussen, J. *Risk management in a dynamic society: A modelling problem*. Safety Science, vol. 17, No 2-3. 1997.

[47] Rasmussen. p. 183-213.

[48] Cilliers, p. 91-92.

[49] Cilliers, p. 93.

[50] Dekker, Cilliers, Hofmeyr. *The complexity of failure: Implications of complexity theory for accident analysis*. Submitted to Safety Science.

[51] Dekker S. *Complicated, complex and compliant: Comments on best practice and colonial patronage in health care*. Submitted.

[52] Reason J. *Managing the risks of organizational accidents*. Ashgate, Aldershot, England, 1997.

[53] Hudson PTW, Reason JT, Wagenaar WA, Bentley PD, Primrose M, Visser JP. *Tripod Delta: Proactive approach to enhanced safety*. Society of petroleum engineers, 1994.