LANDING ACCIDENTS INVOLVING FLIGHT OPERATIONS ON CONTAMINATED RUNWAYS; A SYSTEM THEORETIC APPROACH

Thesis work submitted in partial fulfillment of the requirements for the MSc in Human Factors and System Safety

Bjorn Erik Besserudhagen

LUND UNIVERSITY
SWEDEN

Date of submission: 2007-30-10

LANDING ACCIDENTS INVOLVING FLIGHT OPERATIONS ON CONTAMINATED RUNWAYS; A SYSTEM THEORETIC APPROACH

Bjorn Erik Besserudhagen

Under supervision of Dr. John Stoop

ABSTRACT

Accident models form the basis for investigating accidents. Accident models also influences considerations to be taken and methods and techniques to be used in the investigation process. As systems increases in complexity, accident models need to guide accident investigators to consider broader organizational- and contextual factor in their analysis. Several accidents occur without failure of components, and such accidents are stretching the limits of event based accident models. Accident models based on system theory view accidents as a control problem, and accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled by safety constraints.

Flight operations on contaminated runways are associated with a higher level of risk than when operating from dry runways. The degradation of aircraft performance is significant and the methods for measuring the coefficient of friction do not correlate directly to actual aircraft performance. Over the last few years, there have been a number of accidents which involves this particular type of operations, and in this thesis it is argued that the risks involved are not adequately controlled. The application of an accident model based on system theory is used and it is argued that this approach yields insights to better understand the dynamics involved in these accidents.

TABLE OF CONTENTS

TABLE OF FIGURES

1.0 INTRODUCTION

Increasing complexity in safety critical systems has led to the development of a number of novel accident investigation techniques (de Almeida and Jonson 2007). Some of these new techniques guide investigators to look beyond the immediate events leading up the accident and to consider organizational and managerial structures. One of these novel techniques is based on system theory; STAMP (Systems Theoretic Accident Model and Processes) (Leveson 2004) which view accidents as a control problem and models accidents in terms of violation of safety constraints.

The aim of this thesis is to determine whether the application of elements of the STAMP technique can yield insights into the events surrounding accidents, specifically identify change variables through identifying ineffective or missing control restraints. Elements of the STAMP technique will be applied to two accidents involving flight operations on contaminated runways.

Flight operations on contaminated runways carry a higher level of risk than operation from dry runways. Taking of or landing on a runway covered with standing water, slush, snow or ice involves a significant degradation of aircraft braking performance and directional control. Over the years there have been a number of accidents where contaminated runways have been a contributory factor to why accident occurred. During the last 8 years the Accident Investigation Board of Norway has received 24 reports on accidents and incidents related to slippery runways, measuring and reporting of Coefficients of Friction (CF). The coefficient of friction is measured using different types of vehicles and there exists no generic agreed correlation between measured CF and actual aircraft braking performance (e.g. Root 2003).

In 1983 The National Transportation Safety Board (NTSB) issued a special investigation report regarding large airplane operations on contaminated runways (NTSB/SIR 83/02) and several of the findings in this report is similar to findings in later accident reports1. It can be argued that since these accidents continues to occur the risks involved are not adequately controlled, and it also may indicate that new accident models and perspectives may be required to better understand the dynamics leading up to these accidents.

---

[1] Following a landing accident at Chicago Midway Airport the FAA issued a safety alert for operators (SAFO) which required operators to revise their procedures when operating from contaminated runways. (FAA SAFO 06012).

In most cases, accidents on contaminated runways are not a result of component failure. But rather the failure of airlines, air traffic control, airport management and aircrew to maintain safe operations during inclement weather. Based on this it can be argued that this type of accidents fit the description of system accidents.

1.1 Motivation for choice of research question

The primary motivation for the choice of subject has been sparked through participation in international work in the area of aircraft performance on contaminated runway and trough personal cooperation with accident investigators. There is a strong international interest with respect to how contaminated runways affect aircraft performance, and both aircraft manufacturers and regulators are stakeholders in this work.

A secondary motivation for choice of subject is to explore the possibility to include the subject in potential further post graduate work.

2.0 METHOD

The research question in this thesis is to determine if an approach based on system theory can add analytical value when analysing two similar accidents using elements from the STAMP technique. Within the format of this thesis it will not be possible to conduct a full STAMP analysis which typically would involve identifying and describing; 1) constraints, 2) hierarchical levels of control, and 3) process models. The analysis will be limited to a theoretical study of the model, and constraint analysis together with a limited analysis of the process model on the operational level. The operational level is labelled as the 'operating processes in figure 2)

2.1 Literature

The literature available on flight operations on contaminated runways is primarily focused on how runway conditions affect aircraft performance, and how performance penalties should be calculated. Most of this literature is intended for airlines and aircraft performance engineers. Some literature can be found on tribolgy, more specifically, about methods for measuring the coefficient of friction (CF) on the runway (cf Klein Paste and Sinha 2006). However, very little literature is available on how measured CF correlates to actual aircraft braking performance. The available literature on accident modelling is comprehensive and this thesis is primarily based on the work conducted by Nancy Leveson.

3.0 USE OF ACCIDENT MODELS IN ACCIDENT INVESTIGATION

Accident models form the basis for investigating accidents. Accident models also influences considerations to be taken and methods and techniques to be used in the investigation process. This also means that the accident model may act as a filter or bias towards considering only certain events and conditions or they may expand activities by forcing considerations of factors that are often omitted (Leveson 2004). It is important to take into consideration that accident models invariably is a simplification of the event or phenomenon it attempts to analyse.

3.1 Objectives of accident analysis

The objective of accident investigation, is to identify and describe the true course of events (what, where, when), identify the direct and root causes or contributing factors to the accident (why), and to identify risk reducing measures in order to prevent future accidents (learning) (Sklet 2002). The accident investigation process consists of a wide range of activities, and in general it involves (1) collection of evidence, (2) analyses of evidence and (3) reporting. Accident investigation in aviation shall adhere to the recommendation outlined in Annex 13 by the International Civil Aviation Organization, while other industries do not follow a specific format with regards to the investigation process.

Sklet (Sklet 2002) have made an overview of 14 accident models commonly used in accident investigation, and point out that in the investigation team, there should be at least one member having good knowledge about the different accident investigation methods, being able to choose the proper methods for analysing the different problems (Sklet 2002).

Comparing accident models is a challenging task as there is no common agreement of definition of concepts which is the case within the field of accident investigation.

3.2 Do we need new approaches to accident modelling?

Earlier accident models view accidents as a result from a sequence or chain of events. Such models are adequate when dealing with accidents which involves component failure and for relative simple systems. However, there are a number of accidents which have taken place without component failure and the increasing complexity of technical systems is stretching the limits of accident models based on event based models. Leveson (2004) argues that (1) fast phase of technological change, (2) changing nature of accidents, (3) new types of hazard, (4) decreasing tolerance for single accidents, (5) increasing complexity and coupling (6) more complex relationships between humans and automation, and (7) changing regulatory and public views of safety, are changes that requires new approaches to accident investigation (Leveson 2004). It can also be argued that the concept of drift into failure, (cf Dekker 2005), which entails an incremental movement to a loss event, can not be adequately analysed by means of event based accident models as these models largely ignore social and organizational factors and adaptation over time.

New accident models will have to overcome the shortcomings of earlier models, and should be able to identify accident factors as well as identifying change variables. This in turn will better enable accident investigators and other to make safety recommendations and devise additional safety constraints.

3.3 Limitations of Event Chain Models

A sequential accident model is typically event based. A sudden, unexpected event initiates a sequence of consequences where the last on is the accident (Hollnagel 2004). The direction of causality is from the unexpected event to the unwanted consequence, while the direction of reasoning is from the unwanted consequence to the unexpected event (ibid.). Accident analysis based on sequential models is usually a search for a specific cause and well-defined cause-effect link (Hollnagel 2004). Sequential accident models are easy to understand and are easy to display graphically as each sequence follow a line of reasoning. The sequential accident models have limited capabilities to explain accidents in more complex systems as the accident rarely correspond to the models assumptions about a well-defined link between the unexpected event and the unwanted consequence. As such event chain models is not suited for analysing accident where there are no component failure.

4.0 SYSTEM THEORY IN ACCIDENT INVESTIGATION

Increasing complexity in systems has resulted in accidents that arise not only from component failure, but also from unexpected and unanticipated interaction among components. Perrow used the term system accident to describe it (Perrow, 1984). The analysis of such accidents needs to apply a modelling technique that goes beyond the immediate events leading up to the accident.

In system theory, systems are viewed as hierarchical structures where each level imposes constraints on the level beneath it. System theory sees accidents as an emergent phenomenon, as something that arises out of the complex of conditions (Hollnagel 2004).

An important development within the theoretic approaches to risk assessment came with the work conducted by Rasmussen and Svedung (Rasmussen and Svedung 2000). At the social and organizational levels of their model, Rasmussen and Svedung use a control-based model of accidents and at all levels they focus on information flow. At each level, however, and between levels, they model the events and their initiation and flow of effects using an event-chain modelling language similar to cause-consequence diagrams (Leveson 2005). This chain of events models is similar to timelines; they describe the way in which a particular incident developed over time2.

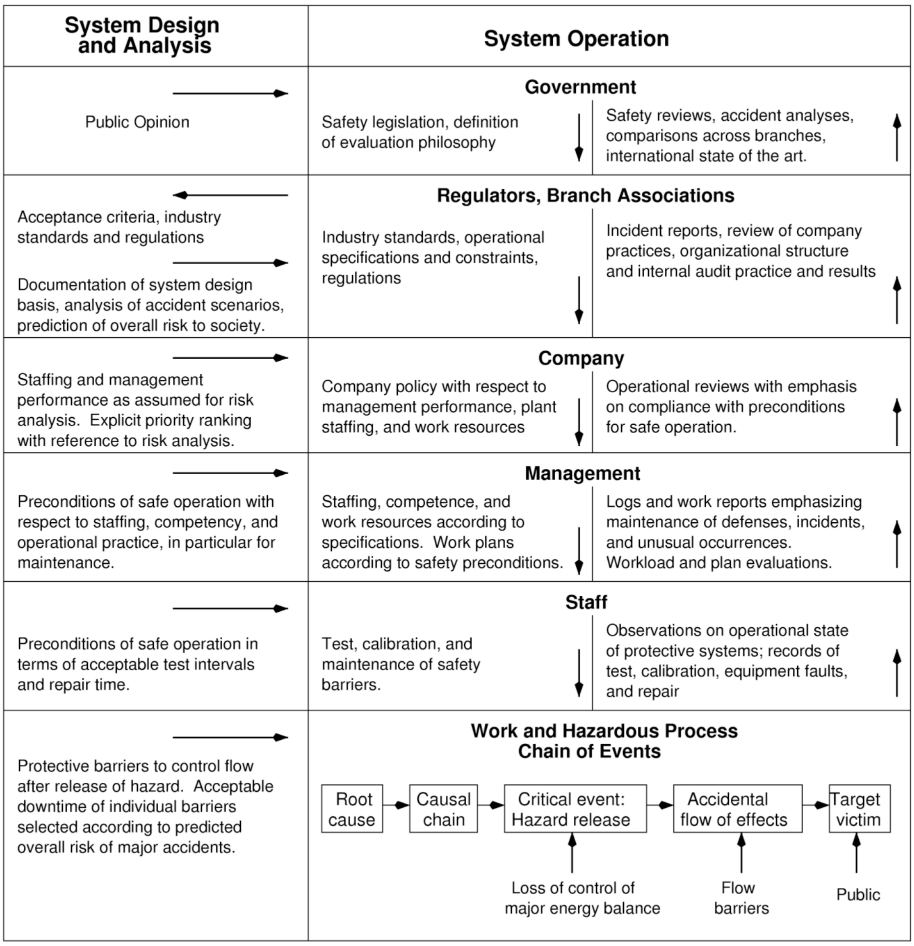

Figure 1

4.1 Theoretic Accident Modelling and Processes (STAMP)

The System Theoretic Accident Modelling and Processes (STAMP) developed by Nancy Leveson (2004) have taken the systems approach one step further by developing a pure systems theoretic model of accident causation. In this model, systems are viewed as hierarchical structures where each level imposes constraints on the level beneath it. Safety is treated as a control problem: accidents occur when component failures, external disturbances, and/or dysfunctional

[2] A comparative study of the Rasmussen model and STAMP has been conducted by de Almeida and Johnson 2007).

interactions among system components are not adequately handled (Leveson 2004). In this context, system theory focuses on how hazards are controlled by adding constraints, rather than adding redundancy.

In STAMP, systems are considered as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. A system is not treated as a static design, but as a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment. The original design must not only enforce appropriate constraints on behaviour to ensure safe operation, but it must continue to operate safely as changes and adaptations occur over time. Accidents, then, are considered to result from dysfunctional interactions among the system components that violate the system safety constraints. The process leading up to an accident can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values (Leveson 2005). The term 'control' should not be understood in terms of a strict control structure, but also in terms of policies, procedures, recommendations and shared values.

STAMP has three fundamental concepts: constraints, hierarchical levels of control, and process models (Leveson 2005), which in turn give rise to a classification of control flaws that can lead to an accident. Leveson suggest the following classification of accident factors, (1) inadequate enforcement of constraints, (2) inadequate execution of control action, and (3) inadequate of missing feedback.

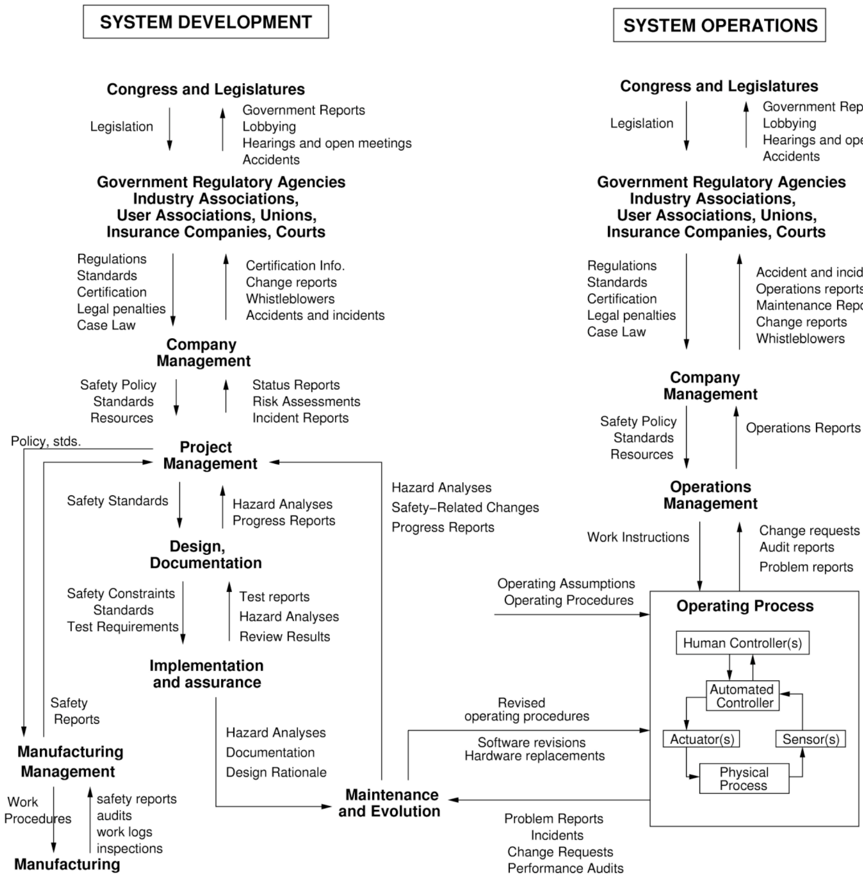

Figure 2

The generic socio technical model of in figure 2 is to some extent similar to the models developed by Rasmussen and Svedung but has two basic hierarchical control structures—one for system development and one for system operation - with interactions between them. Between the hierarchical levels of each control structure, effective communications channels are needed, both a downward reference channel providing the necessary information to impose constraints on the level below and an upward measuring channel to provide feedback about how effective the constraints were enforced (Leveson 2004).

In aviation, the manufacturer has development under its immediate control, but safety involves both development and operational use of the aircraft, and neither can be accomplished successfully in isolation: Safety must be designed into the physical system, and safety during operation depends partly on the original system design and partly on effective control over operations. Manufacturers must communicate to their customers the assumptions about the operational environment upon which their safety analysis and design was based, as well as information about safe operating procedures. The operational environment, in turn, provides feedback to the manufacturer about the performance of the system during operations (Leveson 2005).

4.2 General consideration when applying STAMP

Using STAMP to analyse accidents involves accepting the basic premise in the model that safety is considered as a control problem, and that constraints and feedback mechanisms are necessary to keep the system performance within safety envelope – or in an equilibrium – which is the term used by Leveson. Consequently, accident analysis involves identifying the constraints which were in place and why the constraints where inadequate to control the hazard.

The starting point of a STAMP analysis will usually be a loss event, often referred to as the 'proximal event' in the safety literature. However, the STAMP technique encourages accident investigators to look beyond the loss event and to consider organizational and operational factors which can create a precondition for accident. In fact, it can be argued that most of the potential analytical leverage which can be extracted by applying the STAMP technique may be lost if the analysis is limited to only one level.

It is also important to determine how far the STAMP technique needs to be extended in order to yield findings in an accident investigation. In the literature there is little guidance with regards to defining the 'stopping point' of the analysis, and in most cases it will be impractical to conduct a full scale STAMP analysis due to limitations on available resources.

STAMP must be considered as a primary accident investigation technique in the sense that the technique may be used as the only method. While secondary techniques provide input as supplement to other techniques.

4.3 Practical application of STAMP

In this chapter a STAMP based approach will be used to conduct a comparative analysis of two aircraft accidents which involved landing on contaminated which resulted in the aircrafts departed the end of the runway. These types of accident are commonly referred to as 'overruns'. First, a figure which shows a simplified control loop on the operational level will be presented, and briefly discussed. Second, a constraint analysis of control flaws leading to hazard will be discussed in order to identify missing constraints and / or missing feedback mechanisms.

4.3.1 *The accidents*

Accident 1 took place in December 1999 when a DC 10-103 overran the runway after experiencing very low braking action even though the runway status disseminated by ATIS4 indicted good braking action. The accident investigation board concluded that the measured and reported coefficient of friction (CF) did not reflect actual runway surface conditions.

Accident 2 took place in January 2004 when a DC 10-40F5 overran the runway after experiencing low braking action on the last part of the runway, contrary to runway status disseminated by ATIS that reported low coefficient of friction on the first part of the runway. The accident investigation board concluded that the cause of the accident was that available runway length was insufficient due to contamination and low friction. The flight crew was not adequately informed about the prevailing runway surface conditions

In figure 3 the operation process is presented. The physical process is disturbed when the flight crew experiences braking performance which deviates from what they expected based on the runway conditions reported by ATIS.

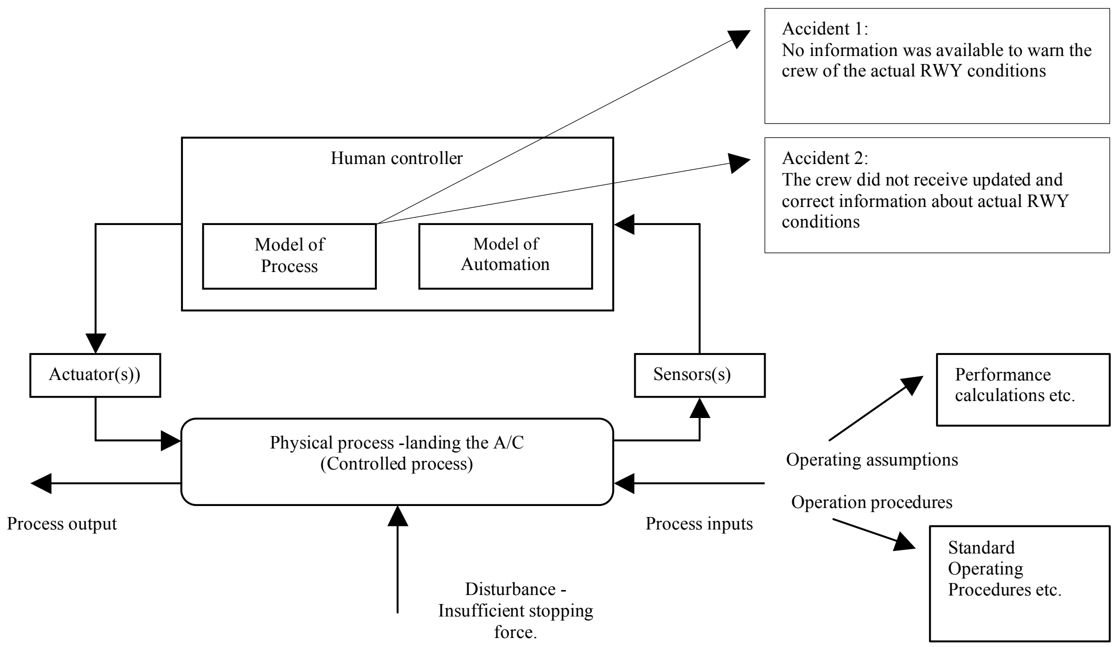

Figure 3

---

[3] Accident Investigation Board Norway, (AIBN) Norway report 2001/05
[4] ATIS is an abbreviation for Aerodrome Terminal Information Service.
[5] Bundesstelle für Flugunfalluntersuchung (BFU), Germany EX0001-0/04, August 2005

For effective control, the process models must contain the following: (1) the current state of the system being controlled, (2) the required relationship between system variables, and (3) the ways the process can change state (Leveson 2005). In both accidents the flight crew's model of process, or mental model, was inadequate due to lack of information about the actual runway surface conditions. It is important to take into consideration that the information about runway status only can be used by the flight crew to make an estimation of expected aircraft braking performance and level of directional control, as there is no generally agreed correlation between reported runway conditions and actual aircraft performance.

On the operation level it can be argued that the model of process was inadequate due to missing feedback mechanisms which left the crew unaware of the current state of the system.

4.3.2 Constraint analysis

The STAMP technique involves identifying missing or inadequate constraints in the system. The general classification constrains are:

Inadequate Enforcement of Constraints
Inadequate Execution of Control Action
Inadequate or Missing Feedback

The table in figure 4 divides the general classification in more detail and provides guidance on the constraint analysis by helping to identify potential causal factors in the control loops that exist at different levels. Leveson (2004) points out that the factors can be applied at all levels, however, the interpretation will differ.

1. Inadequate Enforcements of Constraints (Control Actions)
1.1 Unidentified hazards
1.2 Inappropriate, ineffective or missing control actions for identified hazards
1.2.1 Design of control algorithm (process) does not enforce constraints
- Flaws in creation process
- Process changes without appropriate change in control algorithm (asynchronous evolution)
- Incorrect modification or adaptation.
1.2.2 Process models inconsistent, incomplete or incorrect (lack of linkup)
- Flaws in creation process
- Flaws in updating process (asynchronous evolution)
- Time lags and measurement inaccuracies not accounted for
1.2.3 Inadequate coordination among controllers and decision makers

2 Inadequate Execution of Control Action
2.1 Communication flaw
2.2 Inadequate actuator operation
2.3 Time lag

3. Inadequate or Missing Feedback
3.1 Not provided in system design
3.2 Communication flow
3.3 Time lag
3.4 Inadequate sensor operation (incorrect or no information provided)

Figure 4

On the operational level of the two accidents some possible control flaws leading to the accident can be identified:

1. Inadequate Enforcements of Constraints (Control Actions)	Accident 1	Accident 2
Unidentified hazards Insufficient braking action experienced on landing Reason: Inadequate mental model due to lack of information.	Good braking action reported	RWY conditions not adequately reported
2 Inadequate Execution of Control Action		
2.1 Communication flaw Information about potential uncertainty of measured CF values was not disseminated. Reporting format not adhered to.	N/A	Error in reported CF
3. Inadequate or Missing Feedback		
Aerodrome operator continued to report measured CF even though measurement did not reflect actual conditions.	Did not provide other relevant information	N/A

Figure 5

The following constraint analysis is limited to the activities associated with measured and reported CF and the correlation with actual aircraft performance.

1. Inadequate Enforcements of Constraints (Control Actions)
Inappropriate, ineffective or missing control actions for identified hazards No correlation has been established between CF measuring vehicle and aircraft performance. Missing constraint. No correlation has been established between different types of CF measuring vehicles. Missing constraint due to lack of harmonization.
Design of control algorithm (process) does not enforce constraints No correlating established between measured and observed runway surface conditions and other relevant sources of information, for instance pilot reports.
2 Inadequate Execution of Control Action
2.1 Communication flaw ATIS and the reporting format for runway surface conditions do not provide information about actual runway surface condition to air crew in a timely manner.
2.3 Time Lag Time from observation to reporting may leave information about runway surface conditions invalid.
3. Inadequate or Missing Feedback
3.1 Not provided in system design No universal and reliable values for measured FC established. Operators may lack awareness of the uncertainty of FC measurements.

Figure 6

This constraint analysis indicates that missing and ineffective safety constraint can be identified, and some of the missing constraint was not apparent in the accident reports.

5.0 DISCUSSION

The use of STAMP encourages accident investigators to take a more holistic or integrated approach to the investigation process. The full potential of STAMP is not shown in this thesis, and only a limited analytical leverage can be extracted in the examples used. This has to do with the particular problems associated with these types of accidents and is not due to lack of explanatory power of the STAMP technique. However, but it can be asserted that the technique can help clarify the interaction between different actors in an accident. Studies show that application of novel techniques helped to identify areas that did not receive sustained attention within the official accident documentation (de Almeida and Johnson 2007). The STAMP technique can yield insights into the events surrounding accidents through identifying ineffective or missing control restraints. The constraint analysis can also identify the effectiveness on of reference and measuring channels between different levels, for instance between the operational level and operations management.

Leveson has demonstrated the use of STAMP on several different accidents, and it is safe to say that the technique is a powerful tool when it comes to explaining accidents. However, more work is needed to asses STAMP in terms of a tool for generating system adaptation strategies. Change variables can be identified by STAMP through constraint analysis, which in turn provides guidance about which hazards that need to be controlled.

STAMP seems to overcome several of the shortcomings of event based models, as it does not model only the events leading up to the accident but rather guides investigators to explore variables which are not immediately apparent and includes contextual factors. This is an important factor when working with accidents resulting from drift into failure, where constraint analysis may help identify how constraints was eroding or otherwise became ineffective to control the hazard – in STAMP this may be identified as asynchronous evolution.

Leveson provides limited guidance as to which extent it is desirable or even necessary to build a timeline when using STAMP. In most cases it would be beneficial to identify the proximity in time between the variables included in the analysis. The generic model presented in figure 2 includes two hierarchical control structures, one for system operation and one for system development with the associated interactions between them. How far the accident analysis need to be extended in order to extract analytical leverage has to be decided based on the accident in question. But when faced with an accident investigation the investigators needs to define the scope of the investigation, including a ‘stopping point’, based on their professional judgement.

With reference to the objectives of accident investigation discussed in chapter 4.1, STAMP must be considered suitable in describing the true course of events leading up to the accident. It adds significant value when it comes to identifying the key actors in an accident and how the actors interacted through the process models and the hierarchical feedback mechanisms. STAMP also has the potential explanatory power to explain why accidents happened. The primary tool for generating change variables is through constraint analysis which aims to identify missing or inadequate safety constraints.

STAMP is a quite complex model and it requires a significant amount of planning in order to take advantage of the full potential of the technique. Sklet (Sklet 2002) points out that in an investigation team, there should be at least one member having good knowledge about the different accident investigation methods, being able to choose the proper methods for analysing the different problems. It can be argued that this holds true for the application of STAMP.

As most accident models STAMP will have to rely on informants to identify the interaction among actors involved in the events leading up to the accident. This can represent a problem when trying to distinguish between actual interactions and imagined interaction, as most informants will be inclined to embellish how the organization operates.

In summary it can be argued that system theory represents a valid approach to accident investigation, and the STAMP model provides a tool for taking a more holistic approach to accident investigation.

6.0 CONCLUSION

In this thesis the potential analytical leverage of STAMP is by no means meant to be exhausted, but enough indicators can be found to support the notion that that a system theory is a valid approach in accident investigation. STAMP provides investigators with a tool which can add significant value to the investigation process.

STAMP is a comprehensive and flexible technique that helps accident investigators to consider a broader range of organizational and contextual factors when faced with an accident investigation. Especially, when dealing with accidents in highly complex systems and in accidents which are not caused by component failure alone.

STAMP also has the potential explanatory power to explain why accidents happened. The primary tool for generating change variables is through constraint analysis which aims to identify missing or inadequate safety constraints. In this thesis only a limited number of missing or inadequate safety constraints could be found. But this is due to the fact that only a very limited analysis was conducted.

7.0 DISCLAIMER

The views and ideas expressed in this thesis only reflect the author and shall not be considered as official view of any organization to which the author belongs.

8.0 REFERENCES

Accident Investigation Board Norway (AIBN). (2001) Norway report 2001/05 (Norwegian text)

Bundesstelle für Flugunfalluntersuchung (BFU), Germany EX0001-0/04, August 2005, German text).

Dekker, Sidney (2005): *Then Questions About Human Error: A New View of Human Factors and System Safety*, Lawrence Erlbaum Associates.

de Almeida, Ildeberto Muniz and Jonson, Chris (2007): *Extending the Borders of Accident Investigation: Applying Novel Analysis Techniques to the Loss of the Brazilian Space Programme's Launch Vehicle VLS-1 V03*. Department of Computing Science, University of Glasgow, Glasgow, Scotland. Available for download on: http://www.dcs.gla.ac.uk/~johnson/papers/Public_Policy/US_Blackout_Johnson.pdf

Federal Aviation Administration (2006): *Safety Alert for Operators. Landing Performance Assessments at Time of Arrival.* SAFO 06012, Washington DC

Hollnagel, E (2004): *Barriers and Accident Prevention.* Ashgate

Klein-Paste, Alex and Sinha, Nirmal K (2006): Airport Operations under Cold Weather Conditions: Observations on Operative Runways in Norway. Norwegian University of Science and Technology and National Research Council Canada. Transport Canada Publication No. TP 14648E, Montreal, Candada

Leveson, Nancy (2005): *Safety in Integrated Systems Health Engineering and Management.* NASA Ames Integrated System Health Engineering and Management Forum (ISHEM), Napa, November 2005

Leveson, Nancy (2004): *A New Accident Model for Engineering Safer Systems.* Safety Science, Vol. 42, No. 4, April 2004.

National Transportation Safety Board (1983): *Large airplane operations on contaminated runways.* Special investigation report (NTSB/SIR 83/02), Washington DC.

Perrow, Charles (1984). *Normal Accidents*, Basic Books (reprinted in 19XX by XXX University Press).

Rasmussen, Jens and Svedung, Inge (2000). *Proactive Risk Management in a Dynamic Society,* Swedish Rescue Services Agency.

Root, Rob (2003) *Brake Energy Considerations in Flight Operations*. Boeing Flight Operations Engineering. Seattle, Washington. (Restricted distribution).

Sklet, Snorre (2002): *Methods for accident investigation*, Report no. ROSS (NTNU) 200208, Norwegian University for Science and Technology, Trondheim, Norway. ISBN 82-7706-181-