Having a New Pair of Glasses
Applying Systemic Accident Models on Road Safety

by

Yu-Hsing Huang

Linköping University

Department of Computer and Information Science
Linköpings universitet
SE-581 83 Linköping, Sweden

Linköping 2007
ABSTRACT

The main purpose of the thesis is to discuss the accident models which underlie accident prevention in general and road safety in particular, and the consequences of relying on a particular model have for actual preventive work. The discussion centres on two main topics. The first topic is whether the underlying accident model, or paradigm, of traditional road safety should be exchanged for a more complex accident model, and if so, which model(s) are appropriate. From a discussion of current developments in modern road traffic, it is concluded that the traditional accident model of road safety needs replacing. An analysis of three general accident model types shows that the work of traditional road safety is based on a sequential accident model. Since research in industrial safety has shown that such model are unsuitable for complex systems, it needs to be replaced by a systemic model, which better handles the complex interactions and dependencies of modern road traffic.

The second topic of the thesis is whether the focus of road safety should shift from accident investigation to accident prediction. Since the goal of accident prevention is to prevent accidents in the future, its focus should theoretically be on how accidents will happen rather than on how they did happen. Despite this, road safety traditionally puts much more emphasis on accident investigation than prediction, compared to areas such as nuclear power plant safety and chemical industry safety. It is shown that this bias towards the past is driven by the underlying sequential accident model. It is also shown that switching to a systemic accident model would create a more balanced perspective including both investigations of the past and predictions of the future, which is seen as necessary to deal with the road safety problems of the future.
In the last chapter, more detailed effects of adopting a systemic perspective is discussed for four important areas of road safety, i.e. road system modelling, driver modelling, accident/incident investigations and road safety strategies. These descriptions contain condensed versions of work which has been done in the FICA and the AIDE projects, and which can be found in the attached papers.
To those who supported me
CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>i</td>
</tr>
<tr>
<td>CONTENTS</td>
<td>v</td>
</tr>
<tr>
<td>APPENDED PAPERS</td>
<td>ix</td>
</tr>
<tr>
<td>ACRONYMS</td>
<td>xi</td>
</tr>
<tr>
<td>1 INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 How We See Accidents</td>
<td>3</td>
</tr>
<tr>
<td>1.1.1 An aircraft crashed on a partially closed runway during takeoff</td>
<td>3</td>
</tr>
<tr>
<td>1.1.2 Accident description types (accident models)</td>
<td>6</td>
</tr>
<tr>
<td>1.1.3 Suggested countermeasures</td>
<td>8</td>
</tr>
<tr>
<td>1.1.4 A multi-vehicle crash near a toll plaza</td>
<td>9</td>
</tr>
<tr>
<td>1.1.5 Suggested countermeasures</td>
<td>11</td>
</tr>
<tr>
<td>1.1.6 A multi-vehicle crash at Glen Rock</td>
<td>11</td>
</tr>
<tr>
<td>1.1.7 Suggested countermeasures</td>
<td>13</td>
</tr>
<tr>
<td>1.2 Pros and Cons of a Simplified Accident Process</td>
<td>14</td>
</tr>
<tr>
<td>1.3 Research Purpose and Scope</td>
<td>15</td>
</tr>
<tr>
<td>1.4 Research Background and Approach</td>
<td>16</td>
</tr>
<tr>
<td>1.5 Terminology</td>
<td>18</td>
</tr>
<tr>
<td>2 THEORETICAL BACKGROUND</td>
<td>19</td>
</tr>
<tr>
<td>2.1 New Developments</td>
<td>21</td>
</tr>
<tr>
<td>2.1.1 Normal Accident Theory</td>
<td>21</td>
</tr>
<tr>
<td>2.1.2 Cognitive Systems Engineering</td>
<td>22</td>
</tr>
<tr>
<td>2.1.3 Joint Cognitive Systems</td>
<td>23</td>
</tr>
<tr>
<td>2.1.4 Control and context</td>
<td>24</td>
</tr>
<tr>
<td>2.2 Summary</td>
<td>26</td>
</tr>
</tbody>
</table>
3 THE CHARACTERISTICS OF MODERN ROAD TRAFFIC

3.1 The Changes of Road Traffic

3.1.1 Continuously expanding of road traffic

3.1.2 Increasing demand for safer road traffic

3.1.3 Extended use of information technology

3.2 Toward Complex and Dynamic Road Traffic

3.2.1 Complex and coupled road traffic system

3.3 The Current Approaches to Road Safety

3.3.1 Driver-vehicle-road interaction

3.3.2 Hierarchical road safety management

3.3.3 Road safety program

3.3.4 Intelligent integrated road safety system

3.4 Summary

4 ACCIDENT MODELS AND ROAD SAFETY

4.1 Accident Model

4.1.1 The use of accident models

4.1.2 Attributed causes

4.1.3 System decomposition

4.1.4 Causality

4.2 Types of Accident Models

4.2.1 Sequential accident models

4.2.2 Epidemiological accident models

4.2.3 Systemic accident models

4.3 The Evolution of Road Safety Paradigms

4.4 The Underlying Accident Model of Current Road Safety

4.4.1 Driver errors as a main cause

4.4.2 Linear accident process

4.4.3 Safety measures - eliminating or mitigating “driver errors”

4.5 Summary

5 APPROACHES TO ACCIDENT PREVENTION

5.1 Passive accident prevention approach

5.2 Proactive accident prevention approach

5.3 Retrospective Analysis

5.4 Prospective Analysis

5.4.1 Hazard identification

5.4.2 Hazard analysis

5.4.3 Risk analysis
5.4.4 Reliability analysis

5.5 Risk Analysis, Risk Assessment and Risk Management

5.6 Risk Analysis Methods in Road Safety

5.6.1 FMEA and Human FMEA

5.6.2 FTA

5.6.3 SLIM

5.6.4 Traffic HAZOP

5.6.5 DREAM

5.6.6 Traffic Conflict Technique

5.7 Integrated Retrospective and Prospective Analysis

6 DISCUSSION AND CONCLUSIONS

6.1 Accident Modelling for Modern Road Traffic (ref paper I)

6.2 Driving Modelling

6.2.1 Cognitive systems

6.2.2 Disturbances

6.2.3 Examples of driving models based on a systemic perspective

6.3 Causes of Road Accidents (ref papers II and III)

6.3.1 Complex interactions

6.3.2 Deviation

6.4 Road Safety Strategy (papers II and III)

6.4.1 System turning and accident prevention

6.4.2 Minimize mismatch

6.4.3 Reduced mismatch through JDVRS support

6.4.4 Reduced mismatch through lowered environment demands

6.5 Proactive Road Safety Approach (paper IV)

6.6 Future Research

6.7 Concluding Remarks

REFERENCES

APPENDED PAPERS


**ACRONYMS**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABS</td>
<td>Anti-lock Braking System</td>
</tr>
<tr>
<td>ACC</td>
<td>Adaptive Cruise Control</td>
</tr>
<tr>
<td>AIDE</td>
<td>Adaptive Integrated Driver-vehicle interface</td>
</tr>
<tr>
<td>ATIS</td>
<td>Automatic Terminal Information Service</td>
</tr>
<tr>
<td>ATM</td>
<td>Air Traffic Management</td>
</tr>
<tr>
<td>ASA</td>
<td>Automatic Slack Adjuster</td>
</tr>
<tr>
<td>CKS</td>
<td>Chiang Kai-Shek International Airport</td>
</tr>
<tr>
<td>CSE</td>
<td>Cognitive Systems Engineering</td>
</tr>
<tr>
<td>DREAM</td>
<td>Driver Reliability and Error Analysis Method</td>
</tr>
<tr>
<td>DVE</td>
<td>Driver-Vehicle-Environment</td>
</tr>
<tr>
<td>DVR</td>
<td>Driver, Vehicle and Road</td>
</tr>
<tr>
<td>ETA</td>
<td>Event Tree Analysis</td>
</tr>
<tr>
<td>FICA</td>
<td>Factors Influencing the Causation of incidents and Accidents</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure Modes and Effects Analysis</td>
</tr>
<tr>
<td>FTA</td>
<td>Fault Tree Analysis</td>
</tr>
<tr>
<td>HAE</td>
<td>Host, Agent and Environment</td>
</tr>
<tr>
<td>HARRS</td>
<td>High Accident Rate Road Section</td>
</tr>
<tr>
<td>HAZOP</td>
<td>Hazards and Operability Analysis</td>
</tr>
<tr>
<td>HCI</td>
<td>Human-Computer Interaction</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>HERMES</td>
<td>Human Error Risk Management for Engineering System</td>
</tr>
<tr>
<td>HFACS</td>
<td>Human Factors Analysis and Classification System</td>
</tr>
<tr>
<td>HMI</td>
<td>Human-Machine Interaction</td>
</tr>
<tr>
<td>ICAO</td>
<td>International Civil Aviation Organization</td>
</tr>
<tr>
<td>ILS</td>
<td>Instrument Landing System</td>
</tr>
<tr>
<td>ISA</td>
<td>Intelligent Speed Adaptation</td>
</tr>
<tr>
<td>JCS</td>
<td>Joint Cognitive System</td>
</tr>
<tr>
<td>JDVRS</td>
<td>Joint Driver-Vehicle-Road System</td>
</tr>
<tr>
<td>MTO</td>
<td>Man-Technology-Organization</td>
</tr>
<tr>
<td>NTSB</td>
<td>National Transportation Safety Board</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>PFD</td>
<td>Primary Flight Display</td>
</tr>
<tr>
<td>PSF</td>
<td>Performance Shaping Factor</td>
</tr>
<tr>
<td>PVD</td>
<td>Para-Visual Display</td>
</tr>
<tr>
<td>SLI</td>
<td>Success Likelihood Index</td>
</tr>
<tr>
<td>SLIM</td>
<td>Success Likelihood Index Method</td>
</tr>
<tr>
<td>STRADA</td>
<td>Swedish TRaffic Accident Data Acquisition</td>
</tr>
<tr>
<td>TCT</td>
<td>Traffic Conflict Technique</td>
</tr>
<tr>
<td>WYFIWYF</td>
<td>What You Find Is What You Fix</td>
</tr>
<tr>
<td>WYLFIWYF</td>
<td>What You Look For Is What You Find</td>
</tr>
<tr>
<td>WYSIWYG</td>
<td>What You See Is What You Get</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

To most people, Friday evening is the time to go to a pub with friends or watch a film at home. It should be relaxing and enjoyable. To my family, Friday evening is a “high risk” evening. My three year old son and I form a faithful audience to a special program series broadcasted by the National Geographic Channel every Friday evening. You may wonder how watching TV can become a high risk event, especially on an educational channel. Well, it is because the programs go into detail about the world's most infamous disasters, e.g. the space shuttle Challenger accident, the mid-air collision over Germany, the Paris’s subway accident, and so forth, all of which had catastrophic consequences.

What attracted me to these programs in the first place are not the actual descriptions of the accidents, but the explanations offered of why they happened. To keep the attention of the audience, all programs follow the same pattern of telling a fascinating story. First, an accident and its immediate consequences are presented. Second, the program follows the steps of the investigators as facts about the accident development are gradually uncovered. Finally, once a root cause has been identified, the accident development is replayed from its root cause to the consequences.

Although I know that the common practice in accident investigation and prevention it tries to establish an interlinked chain of abnormal events leading to an accident (like a set of domino bricks falling), I was still surprised by how widespread and embedded this way of understanding accidents is. It dominates accident investigation and prevention in many areas, such as air, railroad and marine traffic. The interviewed experts in the programmes said clearly that the accidents developed through a chain of events and can be avoided if the chain of events is broken.
Since I do not believe the domino brick paradigm is a good one, I was very irritated with these experts until my son asked me a question. As it happened, I had bought my son a pair of sun glasses from a supermarket during a Friday evening food shopping. He had wanted to have a pair of glasses for a while, because he wanted to look like his father (I wear glasses). That evening, when we were watching the “high risk Friday” programme, he put them on for the first time. Then he asked “Why is the light switched off?” His question made me laugh, and I said: “The light is on. It is dark because you are wearing a pair of sun glasses.” This reply didn’t satisfy him, however. Instead he said: “But you wear a pair of glasses too.” I suddenly realized that he had asked me a serious question. I had to think for a while, before I found a reply. I said “Well, I do wear a pair of glasses, but have you noticed the difference between your glasses and mine? Your glasses are dark but mine are clear. We see things differently because we have different pairs of glasses.”

When saying this, I realised I didn’t have to be annoyed with the experts in the programmes. Because we see accidents and foresee probable accidents in accident investigation and prevention through a pair of glasses, wearing a different pair will naturally alter the picture we see. They investigators in the programme were not wrong in any absolute sense, they were just wearing a different pair of glasses. Actually, for every type of investigation that requires conclusions to be drawn, the investigator wears a pair of glasses in the sense that certain information is automatically filtered away as unimportant or unrelated. This is in one way very efficient, because it reduces the complexity of accidents and forces us to see certain things that may otherwise be omitted. In another way it poses a great risk. Accident prevention is about generating countermeasures for accident processes and causal factors found in the accident investigation. If the glasses we wear filter away factors or processes which are truly important to a situation, then our preventive work for that situation will be inefficient at best, and useless at worst.

The pair of glasses described above is obviously not worn on your head but in your mind. They form a personal philosophy of accident occurrence and prevention (Heinrich et al., 1980). This can also be called an accident model; something which guides what we look for and what we foresee in our investigations.

The importance of having a suitable accident model came into focus in the studies of complex systems after the occurrence of a series of catastrophic accidents in the 1980s. Some researchers in this area became very aware of the need for suitable
accident models, and budget and man years have been dedicated to the problem. As a result, a number of accident theories and models have been proposed since then. These new theories and models provide new views on accident investigation and prevention in mainly industrial safety. However, they have not propagated to other areas as much as could be hoped for. Not until recently have they become a topic in areas such as medical treatment, air, railroad and marine traffic operations. This thesis is one of the attempts to bring the lessons learned in industrial safety to bear on the area of road traffic operation. Let’s have a new pair of glasses for the investigation of road crash problems.

1.1 How We See Accidents

An aircraft crash and two road accidents are presented in this section. The purpose of presenting these accidents is to illustrate how we commonly see accidents. The information regarding the accident was retrieved from reports published by the Aviation Safety Council, Taiwan in 2002 (ASC, 2002) and by National Transportation Safety Board in 2006 (NTSB, 2006a, 2006b). These reports provide rather detailed information about the occurrence of the accidents, the findings of the accident investigation, and safety recommendations.

1.1.1 An aircraft crashed on a partially closed runway during takeoff

Singapore Airlines Flight SQ006 taxied onto a runway which was closed due to construction work, and crashed into the construction equipments as it took off at the Chiang Kai-Shek (CKS) International Airport in Taiwan on the night of 31 October, 2000. The accident killed 79 passengers and 4 of the cabin crew.

There were three parallel runways at the CKS airport including one redundant runway. Runway 06 is located at one side of the terminal buildings and runway 05R and 05L are located at the other side. Runway 06 and 05L were equipped with instrument landing systems (ILS), but were authorized for different operation categories. Runway 06 had status as instrument landing category one (CAT I) and runway 05L was an instrument landing category two (CAT II) runway. A CAT II runway (like 05L) allows an airplane to takeoff or land at lower visibility than a CAT I runway (like 06)\(^1\). The third runway, runway 05R, was a redundant and

\(^1\) During a takeoff operation, the requirement of minimum runway visual range at ground level is 550 meters for a category one system and 350 meters for a category two system.
takeoff only runway. It was therefore not equipped with ILS and was normally used as a taxiway. On the evening of the accident, runway 05R was partially closed due to construction work.

Two changes were made and agreed upon by the flying crews\(^1\) in the takeoff operation. Both changes were mainly due to a worsening weather condition causing by an approaching typhoon. The first change was of which pilot should be in charge of the takeoff operation. The takeoff was initially planned to be lead by the first officer, but this way changed to the captain. The change as such is common and reasonable because risky operations are usually led by the more experienced operator if more than one operator is available. In the case of flight SQ006, the captain had much more experienced than the first officer\(^2\). Another change was of the takeoff runway. The takeoff was originally scheduled for runway 06, but the captain decided to use runway 05L instead, due to the poor weather conditions. This decision was also reasonable, because runway 05L has a longer runway and a lower takeoff visibility requirement than the runway 06, due to its higher CAT categorisation.

An ordinary pre-takeoff check was performed during taxi. The crew checked a number of conditions, e.g. engine, rudder, runway, weather and cabin readiness. The results of the pre-takeoff check would decide whether they were allowed to takeoff. Generally, an ordinary pre-takeoff check is a demanding task, and the crew had to put in extra effort during the taxi operation due to the change of takeoff runway. Since the flights of Singapore Airlines normally use runway 06 due to shorter taxing distance, the crew of this flight was unfamiliar with the route leading to the runway 05L. Their navigation to runway 05L therefore depending very much on the airport navigation chart and runway and taxiway signage and markings. Under the very poor visibility conditions, recognition of signs and markings became extremely difficult. While taxing, the crew was also were attempting to get the latest weather information from the Automatic Terminal Information Service (ATIS)\(^3\), as well as listening in on the communication

---

\(^1\) There were three people in the flying crew on flight SQ006: a captain, a first officer and a relief pilot.

\(^2\) At the date of the accident, the captain had accrued a total flying time of 11,235 hours, of which 2,017 hours were on the Boeing 747-400 and the first officer had a total flying time of 2,442 hours, of which 522 hours were on the Boeing 747-400.

\(^3\) Automatic Terminal Information Service is a continuous broadcast of recorded non-control information in busier terminal areas. ATIS broadcasts contain essential information, such as cloud base height, wind speed and direction, visibility, temperature, dew point, the active runway, altimeter settings, and any other information required by the pilots.
between the local controller and two other airplanes which were about to depart. The flying crews were very concerned with getting the latest weather information, because the current conditions just about met Singapore Airline’s takeoff requirement, and if they got any worse, the takeoff would have to be cancelled. Due to the approaching typhoon, this was a likely scenario.

Runway 05L and 05R and the taxiway NP run parallel to each other, and are connected by the taxiway N1 at their one end (see Figure 1.1). To reach runway 05L, the flight SQ006 first had to turn onto taxiway N1 at the end of the taxiway NP. Then, when on taxiway N1, it should pass the first turn (which connects to runway 05R) and make the second turn at the end of the taxiway N1. Unfortunately, flight SQ006 turned immediately after getting onto taxiway N1 and entered runway 05R.

![Diagram of airport layout](image)

**Figure 1.1:** The unserviceable and dim taxiway centreline lights on Taxiway N1. The differences of light setting and marking between Runway 05L and 05R (Adapted from ASC (2002), Figure 1.10-9 & 2.5-3)

When the airplane was turning into runway 05R, the first officer warned the captain that the Para-Visual Display (PVD)\(^1\) was inactivated. At the same time,\(^1\) Para-Visual Display is an assistance device which provides guidance to runway centerline during ground operations.
the flying crew saw a clear view of an illuminated runway. Since the visibility of the runway was so good, the captain decided to execute the takeoff operation, and they ignored the inactivation of the PVD when the airplane lined up with the runway centreline. Approximately 30 seconds after the takeoff roll commenced, the aircraft collided with a number of objects on the ground, including several concrete barriers and construction devices, on runway 05R.

1.1.2 Accident description types (accident models)

An accident and the reasons for it can be described in many ways. A lot of this thesis is about the relationship between accident descriptions and accident prevention, i.e. how the choice of accident description type, or accident model, influences the way preventive work is carried out. Two main description types or models will be defined and discussed. One can be called the chain of abnormal events type and the other can be called a systemic type. The chain of abnormal events type takes the direct results of what is found in an accident investigation. Accident prevention based on such descriptions focuses on causes and the links between them. The systemic description type covers a wider scope, taking not only the direct results from accident investigations into account but also other sources, e.g. similar accidents and system analysis. Accident prevention based on this approach focuses on the performance of the whole system rather than just the failing parts.

The difference between the two types of accident description can be illustrated by the results from the investigation that was immediately launched by the Aviation Safety Council (ASC), Taiwan. According to the accident investigation report published by ASC, the development of the flight SQ006 accident formed a chain of abnormal events. It began with the aircraft entering the incorrect runway, continued with the crew overlooking that the aircraft was on an incorrect runway, and finally the crew ignored the inactivation of the PVD (see Figure 1.2). The first abnormal event made the occurrence of the subsequent abnormal events possible. The chain of abnormal events gradually brought the aircraft toward an accident. Each abnormal event was regarded as the result of an operator’s error. In this perspective, the causes of the accident therefore can be described as a series of operator erroneous actions.
Aircraft on incorrect runway → Incorrect runway overlooked → No PVD ignored → Accident

Figure 1.2: A chain of abnormal events description - the abnormal events and their related human erroneous actions of the flight SQ006 accident

To further explain these operator erroneous actions, a number of contributing factors were identified in the report, such as the poor weather condition and the inadequate airport infrastructure and unclear controller’s instructions which made the crew lose their situation awareness. If we are to illustrate the accident with a systemic description type, then these factors need to be included in the description as well. A description of that type would look like Figure 1.3.

Figure 1.3: The causes of the flight SQ006 accident from a systemic perspective

The accident investigation report published by ASC concluded that the probable causes of the accident were a series of erroneous actions made by the flying crew and several other risks, such as inadequate airport infrastructure, unclear controller instructions, incomplete aircraft takeoff procedures in poor weather conditions and a loss of situation awareness of the flying crew.
1.1.3 Suggested countermeasures - eliminating or constraining pilot’s erroneous actions

In order to learn lessons from an accident, an accident investigation report usually comes with a number of safety recommendations, and this report is no exception. A number of these are listed below. Following each recommendation, I have added a note to point out the event it refers to, the problem it is addressing and what type of countermeasure it is.

To Singapore Airlines:

1. “Ensures that flight crews consider the implications of relevant instrument indications, such as the PFD and PVD, whenever the instruments are activated, particularly before commencing takeoff in reduced visibility conditions.” (No PVD ignored event, human erroneous action, constraint measure)

2. “Include in all company pre-takeoff checklists an item formally requiring positive visual identification and confirmation of the correct takeoff runway.” (Aircraft on incorrect runway event, human erroneous action, constraint measure)

To the Civil Aeronautics Administration, Taiwan:

1. “Immediately implement all items, or acceptable alternative standards, at CKS and other Taiwan airports, which currently are not in compliance with ICAO standards and recommended practices and applicable documents.” (Aircraft on incorrect runway event, human erroneous action, elimination measure)

2. “Establish a reliable incident reporting system, promote the system to the user groups, and place higher priority on the use of such a system.” (Aircraft on incorrect runway event, human erroneous action, elimination measure)

To the Boeing Company:

1. “Consider incorporating cockpit surface guidance and navigation technologies, such as electronic moving map display, into all proposed and newly certified aircrafts.” (Aircraft on incorrect runway event, human erroneous action, elimination measure)
From reading the recommendations, it is clear that the investigators wish to prevent similar accidents by removal of the abnormal events, with a focus on human erroneous actions. The measures of removal are either elimination of human erroneous actions or constraining the effect of human erroneous actions. Little or no though is given to a more systemic perspective.

1.1.4 A multi-vehicle crash near a toll plaza

The following is a description of a multi-vehicle crash near a toll plaza in USA, which was investigated by National Transportation Safety Board (NTSB).

On October 1, 2003, a multivehicle accident occurred on the approach to an Interstate 90 (I-90) toll plaza near Hampshire, Illinois. About 2:57 p.m., a 1995 Freightliner tractor-trailer chassis and cargo container combination unit was traveling eastbound on I-90, approaching the Hampshire–Marengo toll plaza at milepost 41.6, when it struck the rear of a 1999 Goshen GC2 25-passenger specialty bus. As both vehicles moved forward, the specialty bus struck the rear of a 2000 Chevrolet Silverado 1500 pickup truck, which was pushed into the rear of a 1998 Ford conventional tractor-box trailer. As its cargo container and chassis began to overturn, the Freightliner also struck the upper portion of the pickup truck’s in-bed camper and the rear left side of the Ford trailer. The Freightliner and the specialty bus continued forward and came to rest in the median. The pickup truck was then struck by another eastbound vehicle, a 2000 Kenworth tractor with Polar tank trailer. Eight specialty bus passengers were fatally injured, and 12 passengers sustained minor-to-serious injuries. The bus driver, the pickup truck driver, and the Freightliner driver received minor injuries. The Ford driver and codriver and the Kenworth driver were not injured.

The National Transportation Safety Board determines that the probable cause of the accident was the failure of the Freightliner truck driver, who was operating his vehicle too fast for traffic conditions, to slow for traffic. Contributing to the accident was the traffic backup in a 45-mph zone, created by vehicles stopping for the Hampshire–Marengo toll plaza. The structural incompatibility between the Freightliner tractor-trailer and the specialty bus contributed to the severity of the accident (NTSB, 2006a).

The accident process started with a traffic backup in a 45-mph zone caused by a queuing of a toll plaza (see Figure 1.4). The queuing, according to the report, was
a consequence of the toll plaza designer failure to consider the large number of vehicles needing to pass the toll plaza. Next failure was the truck driver maintaining a too short headway to the leading bus and also going too fast to have time to brake once he (belatedly) realised there was a queue. This chain of abnormal events gradually leads to accident.

![Diagram of abnormal events and human actions](image)

**Figure 1.4: Chain of abnormal events description - the abnormal events and their related human erroneous actions in the toll plaza accident**

For an event to be regarded as abnormal there must be a particular and unusual reason for it. As seen in Figure 1.4, human erroneous actions are regarded as the reasons for the abnormal events. The search for accident causes usually follow the chain of abnormal events and stop when salient reasons (salient to the investigators anyway) for the abnormal events are identified.

Just as in the previous example however, there are other possible description of the accident. From the systemic perspective, the description would look like Figure 1.5:

![Diagram of systemic description](image)

**Figure 1.5: A systemic description - The cause and contributing factor of the toll plaza accident**

10
1.1.5 Suggested countermeasures - eliminating designer’s and driver’s erroneous actions

NTSB (2006a) provided a number of suggestions for improvements to concerned organizations. The gist of these are the same as for the Aviation Authorities in Taiwan cited previously, that is to say the focus is on elimination or consequence constraining of human erroneous actions. For example:

NTSB suggested that the Federal Highway Administration, the American Association of State Highway and Transportation Officials and the International Bridge, Tunnel and Turnpike Association:

1. “(Cooperate between the three organizations and) develop written guidelines on toll plaza design that provide information on current tolling practices, electronic toll collection strategies and other equipment designed to eliminate queuing at toll plazas and to improve toll road safety.” (On the event of Queue near toll plaza, human erroneous action, elimination measure)

NTSB suggested that the National Highway Traffic Safety Administration:

1. “… require that all new commercial vehicles be equipped with a collision warning system.” (On the event of Driver brakes too late, human erroneous action, elimination measure)

1.1.6 A multi-vehicle crash at Glen Rock

The following is a description of a multi-vehicle crash at Glen Rock, USA, which was investigated by NTSB.

*About 3:36 p.m., eastern daylight time, on April 11, 2003, in the Borough of Glen Rock, Pennsylvania, a 1995 Ford dump truck owned and operated by Blossom Valley Farms, Inc., was traveling southbound on Church Street, a two-lane, two-way residential street with a steep downgrade, when the driver found that he was unable to stop the truck. The truck struck four passenger cars, which were stopped at the intersection of Church and Main Streets, and pushed them into the intersection. One of the vehicles struck three pedestrians (a 9-year-old boy, a 7-year-old boy, and a 7-year-old girl), who were on the sidewalk on the west side of Church Street. The truck continued across the intersection, through a gas station parking lot, and over a set of railroad tracks before coming to rest about 300 feet south of the intersection.*
As a result of the collision, the driver and an 11-year-old occupant of one of the passenger cars received fatal injuries, and the three pedestrians who were struck received minor-to-serious injuries. The six remaining passenger car occupants and the truck driver were not injured.

The National Transportation Safety Board determines that the probable cause of this accident was the lack of oversight by Blossom Valley Farms, Inc., which resulted in an untrained driver improperly operating an overloaded, air brake-equipped vehicle with inadequately maintained brakes. Contributing to the accident was the misdiagnosis of the truck’s underlying brake problems by mechanics involved with the truck’s maintenance; also contributing was a lack of readily available and accurate information about automatic slack adjusters and inadequate warnings about the safety problems caused by manually adjusting them (NTSB, 2006b).

As can be deduced from the description, the accident description follows the same logic as the previous ones, by establishing a chain of abnormal events which are the result of human erroneous actions.

![Diagram](image-url)  
**Figure 1.6**: A chain of abnormal events and their causes of the Glen Rock accident

As previously, it is also possible to describe this accident from a systemic perspective. As previously, a systemic description will differ from the chain of abnormal events type. For example, since the driver did not receive appropriate driving training, the driver will not be blamed for the accident. He did the best he could, given his knowledge. Instead the mechanics and the truck company are identified as the main contributors to the accident.
Figure 1.7: A systemic description - contributing factors to the Glen Rock accident

1.1.7 Suggested countermeasures - eliminating mechanic’s and driver’s erroneous actions

Below are a part of the recommendations from NTSB (2006b) to the related organizations. The suggestions aim to eliminate driver and mechanic erroneous actions. For example:

NTSB suggested the District of Columbia and the 50 States:

1. “Adopt an air brake endorsement for drivers’ licenses that would require training and testing of drivers who drive air brake-equipped vehicles to ensure their proficiency in the operation of air-braked vehicles …” (On the event of No brake, human erroneous action – Driver uses high gear and pump brake, elimination measure)

2. “Include in your truck inspector training courses a module on automatic slack adjusters that emphasizes that manually adjusting automatic slack adjusters is dangerous and should not be done …” (On the event of No brake, human erroneous action – Mechanics manually adjust ASAs, elimination measure)

NTSB suggested manufactures and marketers of automatic slack adjusters:

1. “Revise your product literature to include conspicuously placed wording that clearly states that automatic slack adjusters should not be manually adjusted …” (On the event of No brake, human erroneous action – Mechanics manually adjust ASAs, elimination measure)
1.2 Pros and Cons of a Simplified Accident Process

Accident prevention, simply stated, is to do something now to avoid accidents in the future. In order to prevent probable accidents, accident prevention has to foresee what and how probable accidents will happen.

Foretelling is not a trusted science, so whether the accidents we predict will actually occur in the future is unknown. However, to fight the enemy we at least have to have an idea of who the enemy is. It is the same in accident prevention. To prevent accidents it is necessary to find out as much as possible about the probable accidents of the future. A common way of handling this is to say that the most likely accidents to happen in the future are simply the most frequent accident types of the past. Therefore, by investigating the accidents of the past, we will probably know the mechanisms of the accidents in the future. This logic implicitly states that the most frequent accident processes and contributing factors identified in the past are the ones we will meet in the future as well.

As the introducing examples revealed, the accident process normally looked for and found in these investigations is one which describes the accident as a chain of abnormal events. Describing the accident process in that way, a single chain with chronologically ordered events, is a simplification of the total accident process, because only a limited number of events and their direct causes are described. Practitioners are sometimes aware of this, but regard it as more of strength than weakness of the approach. It simplifies the analysis, while giving results which still are sufficient for developing countermeasures.

Simplifying the accident process in this way is not always possible however, and perhaps not even desirable, for some fields or types of accidents. This was shown
by the in-depth analyses of several catastrophic accidents in the beginning of
1980s. Those investigations revealed that in order to put efficient countermeasures
in place, an improved understanding of the true complexity of the accident process
was necessary. The chain of events description was not a sufficient tool for the
development of countermeasures. This insight pushed the description of accident
processes in that field from simple to comprehensive. However, in many other
areas a simplified accident process is still the underlying model for how accident
investigation and prevention should be carried out, with little discussion of
whether it can lead to efficient countermeasures or not.

1.3 Research Purpose and Scope

The main purpose of this thesis is to discuss the accident description types, or
accident models, which underlie accident prevention, and in which way preventive
work should be carried out. The thesis deals with two main questions:

1. Should road safety move towards more complex accident model, and if so,
   which one?
2. Should the focus of road safety shift from accident investigation to accident
   prediction?

The research which started with the investigation of the catastrophic accidents in
the 1980's has identified several types of accident models. The chain of events
(sequential) model is one type, and epidemiological and systemic accident models
are other types. This raises the question of whether it is necessary for road traffic
safety to follow the development that already has been underway for some time in
industrial safety. Does the area need to start moving towards more complex
accident models, or is the existing one sufficient?

To answer this, a better understanding of accident prevention is needed. In
Chapter 2 therefore, a theoretical background to the area of accident prevention is
given, as well as an overview of some recent theoretical developments which
holds a lot of promise as tools in the future development of accident prevention.

Also, a better understanding of the characteristics of modern road traffic is needed.
The characteristics of modern road traffic are therefore the topic of Chapter 3. The
conclusion from Chapter 3 is that the current approach to road safety has a number
of drawbacks which makes ongoing preventive work more and more incapable of
dealing with the situation. The field of road safety therefore needs change and development.

As Chapter 2 will show, a cornerstone of accident preventive work is the accident model used for both analysis and formulation of countermeasures. The first step towards a change is therefore to scrutinize the accident model used, as well as the available alternatives. Chapter 4 goes through the basics of accident model concepts, as well as which types are available. It finishes with a description and a critique of the accident model currently in use in most road safety work.

Before the final discussion in Chapter 6 of the possibilities and benefits of pushing the accident modelling of road safety in a more systemic direction, the second question posed above needs consideration. Since the mission of accident prevention is to prevent accidents in the future, its focus should theoretically be on how accidents will happen rather than on how they did happen. Despite this, road safety has traditionally put much more emphasis on accident investigation than accident prediction, compared to areas such as nuclear power plant and chemical industries. However, having many accidents to investigate does not automatically mean that this should be the main research activity. Instead it raises the question of whether road traffic safety should move resources from investigations of the past to predictions of the future, to accomplish better prevention measures.

In Chapter 5 it will be shown that the underlying accident model has a strong influence on whether the research focus lies on retrospective or prospective analysis. The traditional sequential accident model in road safety fits very well with the accident investigations of the past, but less well with accident predictions of the future. If road safety would switch accident model, then the research focus would have to be altered as well, towards what is described as an integrated retrospective and prospective analysis (or a proactive approach).

Finally in Chapter 6, the changes, benefits and alterations involved in bringing the systemic accident model perspective to bear on road safety are discussed.

### 1.4 Research Background and Approach

The studies of this thesis are part of two research projects – FICA (Factors Influencing the Causation of incidents and Accidents) and AIDE (Adaptive Integrated Driver-vehicle interface). The FICA project (2002-2005) is a Swedish national project. The project uses the MTO perspective (Man-Technology-Organization; Kecklund, 1998) to improve the understanding of accidents and
their aetiology, in particular the important MTO factors contributing to accidents and incidents. The goal of the FICA project is to develop guidelines or principles for how the next generation of automotive safety systems should be designed. The AIDE project (2004-2008) is a European Union project under the sixth framework programme. The general objective of the AIDE project is to generate the knowledge, methodologies and human-machine interface technologies required for safe and efficient integration of ADAS, IVIS and nomadic devices into the driving environment.

The research approach adopted in the studies of the FICA project and the studies of the AIDE project where the author has been involved have all been based on an assumption that the study of road safety should be based on systemic accident models. The FICA project uses a systemic accident model, adapted to the domain from a model used in industrial safety. The AIDE project is based on a DVE (Drive-Vehicle-Environment) model which is also a systemic (accident) model.

The appended papers are results of studies with the author involved in FICA and AIDE.

- **FICA: Paper I, II, and III**
- **AIDE: Paper IV**

The studies in the FICA project focus on the accident analysis phase (understanding the past). In order to see whether systemic accident models are more suitable than traditional accident models in accident analysis, a comparison of the results from accident analysis work based on the two models is demanded. The studies provide a qualitative rather a quantitative comparison.

- Paper I discusses the demands of modern road traffic, the general accident models in use and a structural problem in the general models.
- Paper II describes an accident analysis method and the study of drivers’ near-misses which were collected by combining driver diaries with focus group discussions.
- Paper III focus on a specific type of accidents (accidents at intersections) and compares the result of an analysis based on a systemic perspective with a similar study based on a traditional accident model.

The studies in the AIDE project focus on the accident prediction phase (predicting the future). A number of analysis methods used in road traffic were studied and
their focus (e.g. technical failure vs. human failure, risk identification vs. risk analysis) were compared.

- Paper IV is based on a case study and illustrates qualitatively the difference between accident predictions based on traditional accident models and predictions based on systemic accident models.

### 1.5 Terminology

Before 1960s, the term road traffic accident was used to refer to an event in which at least one vehicle crashed and a road-user was injured or killed, or property damaged. The term has been avoided in professional literature since then, because the word *accident* implies that crashes occur exclusively due to fate. Practitioners of road traffic safety however prefer to believe that road traffic crashes are caused by something that can be controlled, e.g. driver behaviour, rather than something that is uncontrollable, e.g. bad luck. The word *crash* is therefore dominantly used in road traffic safety literature. However, the term accident is still in widespread use in general public, and also in other research domains where a lot of the background for this thesis comes from. To respect both traditions, both terms will be used in this thesis.

The most widespread term denoting peoples' mistakes is to call them *human error*. Use of this term is unfortunately very associated with guilt and responsibility, and often constitutes an end point of accident analysis, i.e. the analysis stops when someone to blame has been found. To avoid this focus on guilt of individuals, the term *human erroneous action* will be used instead. A synonym for this term listed in Webster's online dictionary is *inaccurate action*. Since inaccuracy only can be determined in relation to a context or background, it shows more clearly that peoples actions are context dependent and usually reasonable or understandable, but may have unwanted and unexpected outcomes.
To deal with the question of how accident prevention should be carried out, there first is a need to understand what accident prevention is about. In this chapter, a theoretical background to the area of accident prevention is given, as well as an overview of some recent theoretical developments that later in the thesis will be brought to bear on road traffic safety.

The accident prevention framework proposed by Heinrich et al. (1980) provides a framework for accident prevention in which three essential concepts of accident prevention are revealed. These concepts include a philosophy of accident occurrence and prevention, a cyclical decision making and control process and the distinction of short-term and long-term safety management considerations.

The most important concept is that accident prevention begins with a basic philosophy or theorem of accident occurrence and prevention. Heinrich et al. pointed out that familiarity with the basic philosophy is a must for every participant in safety work in any area, and stressed that the success of safety work depends on a sound knowledge of the philosophy. The philosophy is a common belief of what an accident is and how and why it occurs. It can also be referred to as an accident model.

The second concept of Heinrich et al’s accident prevention model is that accident prevention is regarded as a cyclic decision making and control process. In order to achieve a desired level of safety, a number of decisions must be made which includes the choice of indicator to be monitored, the selection of data to be collected, the identification of causes and the selection of remedies. Since a desired level of safety normally is not achieved with one decision, a series of decision making processes are therefore repeated until the desired level is reached.
Even when the desired level is reached, the decision and control loop is kept running to ensure that the desired level of safety is maintained.

![Accident prevention model](image)

**Figure 2.1: Accident prevention model (Heinrich et al., 1980)**

Accident prevention contains a cyclical decision making process and the process is to achieve a desired goal. It is therefore quite obvious that accident prevention is a control process. But it is a control process of a system with a very long response time and with very poor feedback.

The third concept of Heinrich et al.’s accident prevention model is the distinction between short-term and long-term safety management considerations. Short-term safety management considerations are the occurrence of accidents, incidents and unsafe acts; long-term safety management considerations are such as company policy making, company climate, and safety programme climate. The purpose of this distinction is to emphasize that accident prevention should cover not only short-term but also long-term problems, i.e. accident prevention should have both an immediate and a long-term approach. According to Heinrich et al., the immediate approach aims at direct control of personal performance and
environment, whereas the long-range approach resorts to instruction, training and education in industrial accident prevention.

2.1 New Developments

The study of accidents traditionally recognizes human failures as the cause of most accidents. This view has been challenged through the occurrence of a series of fairly recent catastrophes. Study of these catastrophes show that the events were so complex that operators as well as managers and designers were neither able to prevent them nor recover from them. This means that such accidents cannot be avoided through elimination of human failures, and all efforts to prevent them will finally be in vain.

2.1.1 Normal Accident Theory

Based on the studies of these complex catastrophes, Perrow (1984) developed what he called the Normal Accident Theory, which states that the occurrence of accidents is actually a normal status for complex systems. Although normal accident theory proposes that the occurrence of accidents is inevitable, it does not mean we should not, or can not, do anything about them. In fact, normal accident theory proposes a shift of focus within accident prevention. Accident analysis should “focus on the properties of systems themselves, rather than on the errors that owners, designers and operators make in running them” (Perrow, 1984, p.63). He concludes that in accident analysis “what is needed is an explanation based upon system characteristics.”

A distinction between component failure accidents and systems accidents is made by Perrow. This distinction is very important, and will recur throughout the thesis. As the name implies, component failure accidents are accidents caused by individual failures of components. Examples are erroneous actions by operators, technology breakdowns, and design flaws. System accidents have the same origin as component failure accidents, but complex interaction and tight coupling between components make them evolve differently compared to component failure accidents.

Accidents normally contain more than one component failure. In a component failure accident, one component failure activates another component failure. A series of component failures finally develop into an accident. The development of the accident is linear and follows an expected sequence. For systemic accidents,
the opposite is quite true. Although systemic accidents initially begin with component failures, complex interactions between components make the accident development unpredictable and unexpected. For example, in complex systems some components have common-mode features, i.e. a component has more than one function. These components, e.g. human operators and computer-controlled machines, have non-linear interactions with other components. It is concluded that the occurrence of accidental events is normal due to the complex interactions between system components.

Coupling represents the degree of dependence between two objects or systems. If two systems are tightly coupled, what happens in one object directly influences what happens in another.

Efficiency is a critical property of tightly coupled systems, such as continuous processing plants. Through time dependent and invariant processes and little slack, they respond quickly and function efficiently. The shortcoming of this tight coupling is that the whole system becomes very sensitive to disruptions in any of its parts or processes. On the contrary, loosely coupled systems, such as schools, have more flexible performance standards, so they can incorporate shocks and failures or pressures for change without destabilization. However, the price paid for this is slower response and less efficient functioning.

Coupling is particularly related to the recovery from an accidental event. In tightly coupled systems buffers and safety devices must be considered and designed into the system well ahead in time. There are few ways to recover an unsafe situation, and the recovery must be performed precisely. The operators must follow a standard recovery procedure, giving the system correct inputs at the right time. As opposed to this, in loosely coupled systems there is a better chance that expedient buffers and redundancies can be found or created, even though they were not planned in advance. In summary, efficiency requires tight coupling, which in turn results in a difficult recovery process should an accident occur. With looser coupling, recovery is easier but efficiency is lost.

2.1.2 Cognitive Systems Engineering

The study of human-machine systems traditionally separates the studied system into two individual parts, the human and the machine. Human-machine interaction, hence, is depicted as a human receiving information from the machine and then generating a responsive action to the machine. The interaction is carried out
through some kind of interface between the human and the machine. In this perspective, if a system fails and there is no obvious technical breakdown, it stands to reason to recognize the cause of the failure as either the interface or the human. The study of human-machine systems therefore tends to focus on inadequate interface design or on human erroneous actions. Preventative measures are interface and human behaviour focused.

In the field of human factors, an important shift occurred some time ago. Whereas “human errors” used to be regarded as main causes of accidents, another view now predominates, stating that “to err is human.” Human erroneous actions are no longer recognized as main causes in themselves, but rather as brought about by a number of contributing factors. As a consequence, the study of human-machine systems has turned solely towards the interface, which is problematic. If accidents are due to a mismatch between human and machine, then accidents can be reduced by minimizing that mismatch. However, by focusing on the interface alone, the mismatch is not reduced, only bridged.

Cognitive Systems Engineering (CSE) is a system approach for the analysis, design, and evaluation of complex man-machine systems. CSE hosts two main concepts which differ from the traditional human factors approach, and thereby avoids running into the problem described above. First, the human and the machine of a man-machine system are viewed as a joint cognitive system rather than two separated entities. Second, the behaviours of the human operator are seen as shaped primarily by the socio-technical context rather than by an internal information processing system.

### 2.1.3 Joint Cognitive Systems

Through the concept of joint cognitive systems, the human-machine system is regarded as a whole, rather than as a system consisting of two separated sub-systems. “Modelling the human operator as a system in itself is not sufficient.” The dynamics and complexity of the interaction “can only be achieved by providing a coupled model of the human-machine system, and by making the models of either part equally rich” (Hollnagel, 1998, p.72).

A cognitive system is a system which can adapt its output to changes in the environment, with the purpose of staying in control of what the system does. Human beings are prime examples. They can walk in a moving train while holding a cup of coffee upright (most of the time anyway). In this sense, a man
and his machine is also a cognitive system. Hence, a joint cognitive system is defined as a system which can adapt itself to changes in the environment, thereby keeping itself in control of its tasks. A driver with a car is also example of such system. In fact, some machines are cognitive systems in their own right. Such systems can carry out certain processes without the intervention of a human operator. An example is an automatically guided vehicle in an assembly factory.

Defining the scope of the joint cognitive system is a very important part in the analysis of man-machine systems from a CSE perspective, since that is what separates the system studied from the environment. The scope of course depends on the purpose of the study. For example, if the intent is to analyse interaction between traffic airliners and ground control, the pilot and the cockpit can be considered as a joint cognitive system, and everything else as environment. If the purpose is to analyze the interaction between aviation authorities and airline companies, then cockpit, pilot, ATM and Company should be defined as the joint cognitive system, and the rest will be part of the environment.

Figure 2.2: Joint cognitive systems (Hollnagel & Woods, 2005)

2.1.4 Control and context

The most common view of a system’s cognition and actions in the field of human factors today is the information processing view. This view is basically what you get if you use computers as a metaphor for the human mind. In this view, cognition is defined as an internal system state of information processing, as in a computer. It is also held that a system’s cognition is essentially reactive, or feedback driven, just as a computer’s main task is to wait for, and then react to, new or altered input. Also, any action the system takes is assumed to be possible to
Analyse and understand on its own, as a singular response to the current situation. This corresponds to the logic of computer programming languages (“if in state x..., then do action y...”). Analysts searching for causes of disturbance in malfunctioning systems from the information processing view therefore tend to focus on locating errors in the presumed internal cognitive mechanisms (programming errors).

The CSE view aims to present a viable alternative to the information processing view. CSE describes the functions of a (joint) cognitive system as a control process. Remaining in control in order to reach one or more goals is what a cognitive system always attempts to do. Control is defined as a cyclic process consisting of goal setting, situation assessment and action (see Figure 2.3). The cycle emphasises that all system actions belongs to a coherent flow of actions rather than constituting single responses. An action is carried out not only in accordance with the present situation; it both builds on previous actions and takes future possible states and/or actions into account. This means that a system’s actions are proactive, aimed toward future goals, most of time. This is called feed-forward control (as opposed to the reactive, feed-back based control in the information processing paradigm).

CSE regards the control process as shaped by two factors; the operator’s goals and the context. In order to control a system proactively, operators must have a model of the controlled system. The model helps the operators predict upcoming

Figure 2.3: Basic cyclic model of control (Hollnagel, 1998)
situations, i.e. the future. Context is what happens in reality. Normally, there always exist smaller or larger mismatches between the predicted outcome from the operator’s model and the context, i.e. what actually happens. Operators therefore have to adapt their behaviours to the context. Hence, human performance is decided by both the operator’s model of the system and the actual context. Operators have alternatives prepared for upcoming situations, and then selection and execution of these is constrained by the context. Almost all the time, the mismatch between model prediction and context is small enough for the operators to successfully adapt themselves to the context. If the mismatch is too large to be adapted to, the operators loose control.

2.2 Summary

Human erroneous actions are traditionally recognized as the main causes of road accidents. Although within the field of human factors there has been a shift from drivers’ erroneous actions to environmental factors, road accident preventative measures are still driver failure focused. This focus on drivers’ failures is adequate if the system analysed is linear. However, as the analysis in Chapter 3 will show, the road traffic system of today is a complex and mostly non-linear system, where accidents occur due to coincidences of several factors. Such accidents are not possible to prevent using only the human failure approach. Therefore, as proposed by Perrow in the normal accident theory, to reduce the number of accidents focus needs to be on system properties rather than component failures, i.e. drivers’ erroneous actions.

Another traditional view, taken by the researchers of human-machine systems, is to regard the system as an assembly of two separate systems. Whenever the systems fail, the accident analysis will point out either human or machine as the cause, i.e. a component failure. However, the advancement of technology has both increased system complexity and shifted the nature of the operator’s task from a mainly mechanical one to a mainly cognitive one. As the analysis in Chapter 3 will show, this holds true for the drivers and vehicles as well. These changes have made the separation of operator and machine inappropriate. Cognition in such environments makes sense only when the human machine system is considered as a whole.

This thesis takes its theoretical grounding in the normal accident theory and the principles of CSE, because as Chapter 3 and 4 will show, a system perspective on
the study of road accidents is needed, and these theories are appropriate tools for this.
3 THE CHARACTERISTICS OF MODERN ROAD TRAFFIC

A paradigm is a set of practices that define a specific discipline during a particular period of time. The set of practices includes observation, description and prediction. An observation is an inquiry into the features of a phenomenon. A description condensed from the observation is a replicable and valid causal explanation. Prediction indicates that the description should be valid not only for the given phenomenon in the past and present but also in the future. The description of a particular period of time declares that a paradigm does not always hold for a specific discipline. A new paradigm is demanded when the phenomenon itself and/or the requirements of the specific discipline undergo massive changes.

It has been observed that man-made systems are becoming increasingly complex and coupled, making the operation of man-made systems complex and dynamic. In complex and coupled systems, accidents become inevitable. Moreover, due to the scale of some systems, accident consequences are potentially catastrophic. Perrow (1984) pointed out that for such systems, a new aim for accident analysis is needed. The purpose of the accident analysis must be to map interactions between component failures rather component failures themselves. Perrow’s innovative view has greatly affected the recent development of system safety, and now it is time to see if the same change of view needs to be applied to road traffic.

3.1 The Changes of Road Traffic

Motorized road traffic has been in use for more than a century. Road safety has been traditionally focused on component failures, especially driver failures in the past decades. However, as the discussion below will show, the road traffic system is now developing in complexity and coupling rather fast, making the driving task
more complex and dynamic. As traditional road safety was not developed to deal with this new traffic system, changes in the approach to road safety are therefore needed. Before discussing which these changes should be however, we first need to understand how the current approach works. It is difficult to change something you do not understand.

3.1.1 Continuously expanding of road traffic

Although air, rail and marine transportation provide faster, cheaper and larger volumes than road traffic, it is still the major transportation mean. In Sweden, it is estimated that 87% of all passenger-kilometres travelled are by road. Also, it is continuously expanding. Total traffic mileage in 2005 was 74.3 billion vehicle kilometres, which is a 16% increase since 1996. The number of vehicles in use (passenger, lorry and motorcycle) has increased from 2.9 million in 1975 to 4.2 million in 2005. Meanwhile, the total length of Swedish roads (98,300 kilometres in 2005) has not increased, at least not in the last three years. The number of vehicles per kilometre of road is increasing, from 48 in 2002 to 51 in 2005 (SRA, 2006).

3.1.2 Increasing demand for safer road traffic

A common accepted philosophy for work in road safety and other areas is that the safety level of the system should remain at least the same when a new system or functionality is added. Following this philosophy, road safety should at least remain the same, measured through for example annual fatality and injury rates. The continuously expanding road traffic however increases not only mobility but also fatalities and injuries. For example, Huang (2005) points out that road safety in Sweden does not live up to the philosophy. Although the number of fatalities has been decreasing since 1970, the number of slightly and severely injured have been increasing since 1981 and 1996 respectively, and the societal costs for the accidents of course follow this trend.

To deal with these problems, the at-least-the-same safety philosophy is no longer adequate. This has been recognized by a number of motorized countries, resulting in a number of more ambitious visions. The Dutch government proposed a policy of road safety, called intrinsic road safety, in 1991. This policy aims to achieve a 50% reduction of fatalities and 40% reduction of injuries in 2010, compared to 1986. The Swedish parliament passed an act called Vision Zero in 1997, which proposed a vision for road traffic where no driver should be killed or severely
injured on Swedish roads (OECD, 2002). The vision of the European Union is to half the numbers of fatalities between 2000 and 2010 (EC, 2001).

3.1.3 Extended use of information technology

These visions are hard to achieve, because our society demands both mobility and safety. If this was not the case, all travel on roads faster than say 5 kph could be outlawed, thereby reaching Vision Zero basically over night. As it is, the increasing mobility will increase fatalities and injuries by sheer increase in exposure, unless further safety measures are introduced. Since the proposed visions have not been reached despite the development of a number of injury preventive measures (seat belts, air bags, etc), high hopes have been placed on accident prevention through information technology. They are expected to improve not only accident avoidance, but also actually enhance mobility.

A number of technologies have and will be deployed in road traffic. The technologies can be categorized into two groups: safety related and non-safety related technologies (OECD, 2003). The safety related technologies aim to avoid “driver errors”, through for example driver status monitoring and collision warning and mitigation (OECD, 2002). The non-safety related technologies aim to improve the efficiency of road traffic, e.g. driving information systems, variable message signs, or the comfort of driving, e.g. adaptive cruise control. An ambitious and final goal is to have autonomous driving (Ulmer, 2001).

3.2 Toward Complex and Dynamic Road Traffic

The increasing number of vehicle per kilometre of road increases the complexity and uncertainty in driving. Driving becomes very demanding from time to time, and many of the demanding situations are unpredictable and therefore surprising. In fact, the situation is more serious than the statistics suggest, because most of new vehicles are added in urban areas and not uniformly across the country.

The road infrastructure is also growing in complexity. Especially when roads are added or redesigned in cities to handle the increasing traffic flow, many constraints apply, e.g. limited space and existing roads. As a result, the road layout is not always “driver-friendly”. When exiting a highway and entering a large city, often you have to make several quick (because the speed of your vehicle and the short distance of following cars) and continuous decisions (because the road leads in more than one direction). Whittingham (2004) provides an example of coping
with a confusing entry of a north-south trunk road near his village during the first few months that he lived in the village. He describes:

To reach the northbound lane of the trunk road, a driver needs to turn right (south) and proceed southbound along the slip road which then turns through 180 degrees to go north. Conversely, to go south along the truck road, the driver must turn north along the slip road, turn right to cross the bridge over the trunk road and then turn right again to proceed down the south-bound slip road on the other side of the trunk road.

3.2.1 Complex and coupled road traffic system

Information technology is gradually deployed in road traffic. The effects of using information technology in road traffic have not been clearly identified. Rumar (1990) pointed out that the introduction of new components (information technologies) increase the complexity of the road traffic system. A vehicle is no longer controlled by the driver alone, but also by the vehicle itself or other vehicles or even by road infrastructure. For example, a vehicle can detect and adapt to speed changes in a leading vehicle through adaptive cruise control, and information on an adaptive message sign may be necessary to help a driver avoid a collision by receiving congestion information.

Road traffic has remained at quite a slow pace in evolution in the past century. Changes usually took a rather long period of time in developing and testing. Once a change was adopted, the design was used for an even longer period of time. Such “static” period allows “troubleshooting” of the new system alone, i.e. the effect of the new system can be estimated and identified in isolation, and appropriate revision can follow. With recent advances in technology, making changes in road traffic become easier and therefore more frequent. For example, engine characteristics can be changed in seconds with remote software updates. Road traffic system is always at a dynamic state. The analysis of road traffic system therefore should be done by covering at least the related sub-systems rather than a sub-system at a time.
3.3 The Current Approaches to Road Safety

3.3.1 Driver-vehicle-road interaction

The study of road traffic usually regards driving as interactions between a driver, a vehicle and a stretch of road. The driver controls the vehicle by receiving information from the vehicle and the road. The vehicle receives control from the driver and information from the road. The road sends out information to the driver and the vehicle. The drive (D), vehicle (V) and road (R) form a DVR unit (Gunnarsson, 1996). Several DVR units operating together constitute the traffic environment.

![Diagram of DVR unit with labels: D = Driver, V = Vehicle, R = Road]

Figure 3.1: A DVR unit contains a driver (D), a vehicle (V) and a stretch of road (R). Driving is regarded as interactions between the three components. The traffic environment is constituted by several DVR units.

In an accident analysis, one DVR unit at a time is usually studied. The study of the behaviours of a DVR unit is based on a linear interaction between the driver, the vehicle and the road (Figure 3.2). The result of an accident analysis is a chain of inadequate behaviours of the components. If a collision contains more than one DVR unit, each DVR unit is studied by itself first, and the relation (interaction) between the DVR units is built after that.
3.3.2 Hierarchical road safety management

Gunnarsson (1996) proposed that the operation of DVR units is only the micro level of a road traffic system. A complete road traffic system also contains two other levels. The meso level is constituted by the psycho-social environment and local physical environment, and the macro level is constituted by society. The micro level is affected by the other two levels, i.e. the performance of DVR units is not only produced by the micro level but also affected by the meso and macro levels of road traffic. From a road safety management point of view, the performance of a DVR unit or the road safety as a whole can be improved by adopting a management (top-down) approach, i.e. the target and problem are defined by the top level and the measures are developed and implemented at the bottom level.

A hierarchical structure of safety management contains a number of layers from top to bottom, including government, regulators, companies, management, staff and work. The highest levels, i.e. the government and regulators, produce laws and regulations to rule the behaviours on the levels beneath them. Those on the middle levels, i.e. the company and management levels, are on one hand requested to follow the laws and regulations, and on the other hand eager to minimize efforts and maximize their performance. At the lowest level are the staffs who are requested to follow not only the laws and regulations from the top levels but also the policies and plans from the middle levels. The staffs, just like the middle levels, also want to minimize their efforts and maximize their performance.

As shown in Figure 3.3, road safety management can be depicted as such a hierarchical structure where road users, vehicles and road infrastructure are three sub-systems.
Based on studies of accidents, including road collisions, Rasmussen & Svedung (2000), points out that safety management of large and complex socio-technical systems in terms of their hierarchical structure is problematic. At each hierarchical layer decisions are made based on specific domain knowledge and considerations to achieve specific goals. Communication is often ineffective and usually one-way and top-down.

Figure 3.3: Accident prevention contains a multilevel of decision makings. The decision makings of each level base on specific domain knowledge and aim to control the level below it. (Adapted from Rasmussen & Svedung, 2000)

3.3.3 Road safety program

OECD (2003) identified a common planning procedure for developing and implementing road safety programmes from experienced and successful OECD countries. The common planning procedure provides a good way to understand road traffic practices systematically. The steps of the common planning procedure are shortly described below and their relation is depicted in Figure 3.4.

- Vision vs. philosophy: Vision or philosophy is the way a government approaches the problem of road safety. The traditional philosophy is to regard road safety as a health problem. Measurements such as annual fatalities, economic consequences, and comparison between modes of
transport are used to indicate the seriousness of the road safety problem. In recent years, more expansive visions have been developed in a number of countries as a new philosophy. A vision is “an innovative description of the future traffic system or a desired direction of safety development”.

**Figure 3.4: The steps of planning procedure for developing and implementing road safety programmes (OECD, 2003)**

- **Target setting**: The selection of problems for analysis and development of countermeasures are closely related to the target of road safety. When road safety is considered as a health problem, target setting usually is done by comparing seriousness between modes of transport and other health problems, effectiveness of available safety measures and socio-economic appraisals. Visions, on the contrary, put target setting at the first place and lead the development of other steps. A list of targets of OECD countries is provided in OECD (2003).

- **Problem analysis**: In order to achieve the selected target, traffic problems need to be identified, i.e. types and causes of collisions. Traditionally the identification of traffic problems is done on the basis of a few years’ statistics. The statistics based on police reports provide limited information.
In recent years, detailed information has been requested by collision analysis. Several data bases based on in-depth accident investigations are being established in countries and EU projects. Besides, problem analysis which passively focus only on the current situation is not always sufficient; problem analysis should proactively prepare for the future, e.g. aging, the introduction of information technology.

- **Measure selection:** Traffic safety measures are aimed at road users, vehicles, road infrastructure and its environments. Three approaches are applied in the planning of measures: decreasing the exposure, decreasing the collision risk and decreasing the risk of fatality or injury. The selection of approaches and measures depends very much on the results of target setting and problem analysis as shown in Figure 3.4.

- **Evaluation and monitoring:** The purpose of this step is to see whether the selected safety measures are effective and only the measures that have proven their worth will be continue to be adopted. A common used method is cost-benefit analysis. Other impacts of the measures, e.g. environmental view, social acceptance, are usually taken into account.

Oppe (1990) pointed out that road safety research usually is based on a data-driven management approach. In road safety, decisions made on the higher levels are based on accident statistics from police reports. The accident statistics can be used as indicators to show the state of road safety but are inadequate developing road safety measures. The national statistics is collected for management purpose but not for research purpose.

### 3.3.4 Intelligent integrated road safety system

In European Union, the current approach for improving road safety is to take an integrated approach towards building an intelligent integrated road safety system. “Human errors” in road traffic are regarded as the main problem of road safety. Therefore, this approach aims to take advantage of information technology and extend autonomous vehicle systems so that “human errors” can be reduced (EC, 2002).

In order to know which function need to be automated and what the effectiveness of the automation will be, the approach promotes building a European wide database of accident causation.
One of the most important building blocks in setting up a strategy for the deployment of intelligent integrated road safety systems into the vehicles is the availability of a European wide database of accident causation data. Only on the basis of clear statistics on the causes of accidents can the impact of new safety systems be evaluated and the real potential of these systems highlighted. Targeted actions can then be formulated, and the deployment accelerated (EC, 2002).

3.4 Summary

The continuously expanding road traffic makes road traffic more complex and dynamic. As the normal accident theory by Perrow shows, accidents become inevitable in such a system. The continuous expansion also amplifies the negative consequences of road traffic. Road safety demands measures that not only reduce the number of fatalities but also the number of injuries and even the number of accidents. Information technology holds a lot of promise in improving efficiency and safety of road traffic. However, the use of information technology will increase the complexity even more.

Current road safety at a micro level studies the interactions between driver, vehicle and road. Attention is focused on making the interactions as reliable as possible, with the driver regarded as the most unreliable component in the triad. At a macro level, road safety is currently seen as a management problem. The targets and problems are defined by the top level, while countermeasures are developed and implemented at the bottom level. Each level in the hierarchy tends to maximize their local performance rather than performance of the system as a whole.

Road safety at both the micro and macro levels is based on a structural description of road traffic. System analysis based on structural decomposition tends to regard component failures as the causes of accidents. Although road safety programs is a functional description of road safety, the structural decomposition of road traffic makes road safety programs focus on component failures.

To be able to analyze road safety in terms of interactions between component behaviours rather than component behaviours, a new paradigm is needed in road safety. The focus of road safety should therefore move from driver failures to system failures.
4 ACCIDENT MODELS AND ROAD SAFETY

As Chapter 2 showed, a corner stone of accident preventive work is the accident model used for both analysis and formulation of countermeasures. The first step towards a change of the preventive work in any area is therefore to scrutinize the accident model used, as well as go through the available alternatives. Chapter 4 gives an overview of the basic accident model concepts, which types are available and the accident model currently in use in most road safety work.

Beneath all accident preventive work there always exists an accident model. The first part of this chapter explains what an accident model is and why it is important in accident prevention.

In the second part of this chapter, accident models for road safety are categorized into three general types. The classification is based on Hollnagel’s classification of accident models (Hollnagel, 2004). The essential characteristics of accident models, i.e. attributed causes, system decomposition and causality, are discussed.

After this discussion, the development of road safety paradigm described by OECD (1997) is reviewed, as well as actual practices in road safety. By comparing paradigms and actual practices in road safety with the characteristics of accident models, the accident model underlying most of existing road traffic safety is identified.

4.1 Accident Model

Accident preventive work always has an underlying accident model and it is usually implicit, which is not to say that it is unimportant. The implicitness is rather a consequence of the accident model having permeated the field it is applied so thoroughly that no one feels a need to describe it explicitly (if they even know
it is there). Accident models are usually inherited rather than selected. They are built on specific technical cultures and shaped by many years’ experience of application. Conditions foster but also constrain the accident models, though this is seldom given thought by the practitioners of the field.

4.1.1 The use of accident models

Heinrich et al. (1980) were the first to point out the existence and importance of accident models as early as in 1930s (although the term accident model was not in use at that time). They propose that there existed a basic philosophy of accident occurrence and prevention shared by the people involved in accident prevention (see the accident prevention model in Figure 2.1).

Accident models are important in accident prevention because they provide a kind of “mental model” and communication tool for persons involved in accident preventive work. The model contains a common pattern which specifies the causes of accidents, and the links between causes and consequences. When the accident investigators collect data and look for causes, they do it in relation to this pattern. There is also a correlation between the accident data collected and the countermeasures generated. For example, if the accident model says operator erroneous actions are the usual causes of accidents, then the investigators’ focus will be on operators’ erroneous actions. Moreover, they will definitely find one or more such actions because they “know” they must exist (otherwise the accident could not have happened, right?). Once they find a series of erroneous actions, measures are taken to prevent them from being carried out again.

This can be summarised by an analogy from the field of Human-Computer Interaction (HCI). What You See Is What You Get (WYSIWYG) is a design principle used in HCI. It says that you should aim to minimise the difference between what is shown on the screen and what the printer actually prints. When this succeeds, users can predict what they will get from the printer by viewing what’s on the screen.

Following this principle, the procedures of accident prevention (both accident analysis and accident prediction) can in their turn be described as What You Look For Is What You Find (WYLFIWYF) and What You Find Is What You Fix (WYFIWYF) (Hollnagel, 2006).
Figure 4.1: Accident prevention and its underlying accident model

4.1.2 Attributed causes

An accident model is a collection of several concepts that relate to the analysis and prediction of negative system performances. These concepts are attributed causes, system decomposition and causality, and they will be discussed in this and the next two sections.

Whenever an accident occurs people are eager to know what caused it. Motives for this are varied. Insurance companies need to assign guilt to settle damage claims, police need to determine if someone should be charged with a crime, and governments or company management want to prevent similar accidents. Besides these apparent purposes, people sometimes want to know the causes of accidents just out of curiosity, especially if the consequences are spectacular.

Regardless of the motives for finding out the causes of an accident, people normally have an opinion on possible and acceptable causes long before the investigation has begun. Such pre-determined or attributed causes have been studied and found to have some interesting properties.

An interesting example is a study which showed that the results and recommendations from an accident analysis were related to both the purpose of the analysis and the analyst’s domain knowledge (Svenson et al., 1999). Two groups, one with engineering students and one with psychology students, were taught an accident analysis method and given the task of analysing a real healthcare accident. They were also informed that in the official investigation, the head nurse was the only one found responsible for the accident, therefore being sentenced to conditional prison and fired from her job.
The results of the study showed that both groups of students attributed the causes of the accident to other agents rather than a single person. It also showed a difference in attributed causes and prevention recommendations between the two groups of students. The group of engineering students found more human factors errors than technical errors in their analysis, and had a preference for technologically based preventive measures compared to human factors based measures. The analysis and recommendations from the group of psychology students was exactly opposite. They attributed more technical errors than human factor errors and recommended relatively more human factors based measures rather than technical based measures. Svenson et al. (1999) concluded that the attributed causes were more dependent on basic profession training and/or motivation, while the modelling of the accident evolution preceding countermeasure recommendation was relatively less dependent.

Hollnagel & Woods (2005) points out that the attributed causes of accidents has evolved from incorrect machine actions to operator erroneous actions and recently to incorrect organization actions.

4.1.3 System decomposition

To attribute a cause of negative system performance, it is necessary to decompose the system into smaller elements, e.g. sub-systems, components and functions. For example, to attribute the cause of a road accident, the road traffic system can be initially decomposed into the driver, the road and the vehicle. The preliminary cause of the crash might be a driver failure, a road infrastructure failure, a vehicle failure or a combination of two or three of the failures. The initial decomposition is however too simple to fulfil the needs in practice. Therefore, further decompositions of identified elements are usually needed. A vehicle is further decomposed into lateral and longitudinal control systems, i.e. steering and braking. The decomposition is usually in terms of the mechanical or functional structure of the system.

4.1.4 Causality

Causality is a description of the relation between two states. The occurrence of state A (the cause) brings about the occurrence of state B (the effect). Causality is important in describing development of accidents. For example, if a following driver does not see the braking lights of the vehicle ahead come on, the driver will
not apply his own brakes. Missing the braking signal of the vehicle ahead is the cause and not breaking one’s own vehicle is the effect.

Inferred causality is used in the analysis of accidents. When searching for the causes of an accident, the analyst usually already has determined a number of possible and/or logical causes or causal chains that could result in negative effects. Some of these will then be eliminated by comparison with collected data. Using the same example, the vehicle remaining at the same speed is the known effect. Causes that can be possibly inferred for this are broken brakes, no brakes applied, or acceleration great than deceleration to name a few. From a strictly logical point of view, an effect can normally be viewed as being caused by any number of factors in combination. In practicality however, the analyst often tries to narrow it down to one and only one cause per effect, which s/he then calls the primary or root cause.

4.2 Types of Accident Models

A number of accident models have been proposed in different areas. Though different in details, they share several common traits. A categorization of the particular accident models into more general ones could therefore improve our understanding in accident prevention (Surry, 1969). Different categorizations of accident models (Surry, 1969; Heinrich et al., 1980; Lehto & Salvendy, 1991; Leveson, 1995; Hollnagel, 2004) target different areas and emphasize specific concepts of accident occurrence and prevention. For example, categorizations made by Surry (1969) and Heinrich et al. (1980) are applied on industrial safety or occupant protection and focus on the generation of unsafe acts by human operators.

The categorization of accident models made by Leveson (1995) and Hollnagel (2004) applies to the safety of complex systems and are both based on a systemic view of function and failure. However, regarding generation and prevention of accidents Leveson focuses on management of complex systems while Hollnagel focuses on the evolution of cognitive systems (Huang, 2006).

Hale (1999) categorized the development of safety over time as three “ages”, where we currently are passing into the third age. While the focus of the first two “ages” has been technical and human failures respectively, the focus of the third “age” is on socio-technical and safety management systems. The focus of this third age is also the focus of this thesis, for two reasons. First, driving is very more
a dynamic job than a routine task. You may, for instance, adopt the same procedures while driving to and back from office every day but you never use the procedures in exactly the same sequence on specific times. Second, the management approach is yet far from effective in large and loose systems, such as road traffic. Much work performed in road traffic is hardly or not controlled, e.g. speeding or drink and driving. It has been said that road traffic will be absolutely safe if all aspects of road traffic were the same as in air traffic, i.e. using only specially selected and trained operators, strict requirements in maintenance and operation and a good incident reporting system and data recording.

For easy comparison between the types of accident models, the discussion of each accident model contains an introduction, and then describes the attributed causes of the model, the scope of model, the accident evolution, the relation between causality and inferred causality, and prevention strategy. Readers interested in details of the accident models are referred to Hollnagel (2004) and Huang (2005).

### 4.2.1 Sequential accident models

Sequential accident models describe the development of an accident as a chain of events and imply that the way to prevent an accident is to break the chain. The earliest and popular sequential accident model is the Domino theory (Heinrich et al., 1980).

![Figure 4.2: The attributed causes of sequential accident models](image)
Attributed causes – human erroneous action

The Domino theory was developed from the study of industrial accidents and concluded that unsafe acts of human operators or unsafe mechanical or physical conditions are the causes possible to attribute to accidents.

Scope – only operation level

Sequential accident models focus on the operation level, especially on operations performed immediately before an accident. The events usually involve the actions of road users and vehicle and road behaviours.

Accident evolution – one chain of events

Events are the essential elements in sequential accident models. An event is something unexpected happening, usually with something abnormal to it. Because the something will not happen just out of blue, there must be another event which caused it. The occurrence of an event is therefore caused by the occurrence of an antecedent event, thereby possibly triggering a subsequent event until a negative and unwanted state is reached. A chain of events can be built by following the causality from one event to another retrospectively (accident analysis) or prospectively (accident prediction), with the domino model normally allowing only one chain to be constructed per accident. However, an event is usually caused by more than one event. The selection of causality depends on the attributed cause. Taking the same example from the analysis of healthcare accident made by engineering and psychology background students, engineering background students regarded human erroneous actions as an attributed cause so that they tended to select the causations which linked to human erroneous actions and vice versa for the psychology background students.

Relation between causality and inferred causality – treated as equal concepts

Causality is the relation between cause and effect(s), where the cause is logically predetermined to precede the effect(s) in time and/or space. To draw certain conclusions on such relationships, the analyst needs to observe first cause and then the effect(s). For accident analysis however, there rarely exists opportunities to study events in that order. The analysis usually begins after the accident has happened, with only the observable effect(s) available for analysis.

Therefore, in accident analysis, it is more fitting to talk about inferred causality. Inferred causality means establishing a relation from an observed effect to its
probable causes. In sequential accident models, conclusions from inferred causality studies are treated with the same dignity as studies of causation proper. If an investigation infers that an effect is due to a certain cause, then it is also believed that if the cause comes up again, the effect will inevitably occur.

Prevention strategy – eliminate attributed causes

In sequential accident models, the principle for accident prevention is to find a suitable way to break the chain of events leading to the accident. As for how to break it, Heinrich et al. (1980) suggests removing unsafe acts and unsafe mechanical or physical conditions.

4.2.2 Epidemiological accident models

Epidemiological accident models compare the occurrence of accidents to a process of disease infection. In disease prevention, a Host-Agent-Environment (HAE) model is used to describe the process of disease infection. An agent (i.e. a virus or similar) can successfully infect a host when a set of matching conditions for the agent, the host and the environment occurs.

Haddon (1972) proposed a strategy for injury prevention based on the HAE model known as Haddon’s matrix. Haddon’s injury prevention strategy has had a huge impact on the development of injury prevention and may be quite familiar to many of the readers. However, injury prevention and accident prevention are two different things. As the epidemiological accident model discussed below is for accident prevention, it is different from Haddon’s matrix.

Attributed causes – active and latent failures

Epidemiological accident models describe the occurrence of an accident as due to a coincidence of latent failures (Environment), active failures (Agent) and a traffic system (Host). Epidemiological accident models can be seen as extended sequential accident models. An accident is triggered through an active failure. Active failures are failures which occur immediately before the accident and the effects are instant, e.g. driver erroneous actions. These active failures are what sequential accident models describe. The epidemiological models however extend beyond the immediate situation by saying that the active failures are natural consequences of so called latent failures. Latent failures are failures which have taken place (long) before the accident happens, such as improper vehicle maintenance or the setting up of confusing traffic signs. If uncorrected, the effects
of latent failures will lay dormant within the system for a long time. An example of taxonomy of latent conditions is the Human Factors Analysis and Classification Method (HFACS; Wiegmann & Shappell, 2003)

**Figure 4.3: The attributed causes of epidemiological accident models**

**Scope – from operation to design levels**

Epidemiological accident models cover a wider scope than sequential accident models. The inclusion of latent failures extends the scope from operation to maintenance and design levels. The scope also can be seen from temporal and spatial sense. Epidemiological accident models cover a scope from here and now to remote places and times.

**Accident evolution – multiple chains of events**

Epidemiological accident models can be seen as extended sequential accident models. The accident evolution is still linear but extended to cover latent failures. From a hierarchical system perspective, the extended scope in time also extends the search for failures from the lower levels to the higher levels of the hierarchy in the road traffic system, and put a demand for countermeasures on these levels. Accident defences both physical (like the development of adaptive cruise control) and non-physical (like regulations) are the actions of higher levels in the road traffic system, e.g. company, regulators and government. The defences are a kind of management tool to ensure the system under supervision can act as planned.
The epidemiological models are also extended in the sense that there can be more than one chain of events leading up to the accident. For instance, in the truck accident described in the introduction, one chain of events leading up to the accident is that the company issued a dispatch which contained a latent failure, i.e. route guidance to the accident downgrade. Another chain of preceding events is where the mechanics repaired the truck brakes incorrectly, and this latent failure remained undetected during normal operation, until the accident occurred.

Relation between causality and inferred causality – treated as equal concepts

Although epidemiological accident models have a more complex accident evolution than sequential accident models, the relation between causality and inferred causality is still as same as for sequential accident models, i.e. causality and inferred causality are treated as equal concepts.

Prevention strategy – strengthen defences

The attributed causes in epidemiological accident modelled are the latent failures, and the strategy for prevention is to establish defences which can prevent latent failures from occurring. In medicine this can be mandatory vaccination, in road safety it can be annual vehicle inspections.

The concept of defence is related to the hierarchy perspective of system management. A road system is decomposed into several layers, where a lower layer is controlled by a higher layer. Defences are established through a higher layer adding a number of barriers to guide or constrain the actions of a lower layer to stay within an acceptable range. A layer itself can be seen as a barrier too, because it can prohibit inadequate control being applied to lower layers. The occurrence of accidents therefore can be regarded as either a consequence of inadequate control in a higher layer or the lack of adequate barriers in a lower layer. This means that although the attributed causes of epidemiological accident models are latent failures, the goal of prevention is not to eliminate the latent failures but to strengthen the defences. This is done by establishing all necessary barriers, i.e. install missing ones and replace inadequate ones.

This strategy of strengthening defences had been adhered to in road safety for both latent failures and active failures. Defences for constraining the consequences of active failures have been developed for more than half a century, starting with injury reduction and recently to going into accident avoidance. Examples of
defences for active failures are seat belt, air bag (injury reduction defences) and automatic speeding cameras and alco-lock systems (accident avoidance defences). Defences for constraining latent failures are road inspections and regular maintenance. However, the ways in which latent failures weaken the defences often receive less attention. Even if the latent failures are identified they often lack effective solutions. Look at the truck accident in the introduction. There exists, for example, defences for preventing an unqualified driver from operating a truck and defences for keeping a heavy truck away from residential areas, but these defences were weakened or disabled by latent failures. The requirement of only qualified truck drivers was disabled by company management, and the traffic signs advising detours for heavy trucks (an active failure defence) was weakened by the dispatch of an inadequate delivery route.

4.2.3 Systemic accident models

Systemic accident models have one major difference from sequential and epidemiological accident models. While the latter describe an accident process as a chain or tree of events, systemic accident models describe an accident process as a complex and interconnected web of events. Systemic accident models emphasize the analysis of a joint system as a whole. Accidents occur when the performance of the joint system cannot meet the requirements of its environment. The performance of the joint system is a result of interactions between all the components of the system. A mismatch between system performance and the requirements of the environment is also an effect of all system components rather than any single component. In the distinction made by Perrow (1984) between accidents caused by component failure and accidents caused by complex interactions between components, systemic accident models focus on the latter. However, the former can be seen as a case of the latter.

Attributed cause – MTO factors

The performance of a system is an ensemble performance of its components. The occurrence of an accident can be seen as a process in which the performance of the system eventually is unable to meet the requirements of the environment. This process towards a mismatch contains a number of unexpected events each caused by a number of events (factors). In Nordics countries, the search for causes of an effect in accident analysis usually aims to find MTO factors (Kecklund, 1998). The MTO concept emphasizes that the occurrence of an event always have more
than one contributing cause or factor, and these factors are stem from a broad spectra of human, technical and organizational factors.

A cognitive system always has a number of goals and tries to achieve these goals by following rather simple rules. The behaviour of a system is the result of complex interactions between its cognitive system and the environmental conditions. In order to achieve a number of goals, feedforward control is very often used to increase the performance of a system. Feedforward control reduces the need for, and efforts involved in, feedback control. The occurrence of an accident is a mismatch between the performance of a system and the demands of the environment.

The mismatch is due to a cognitive system failing in both feedforward and feedback control and one or more unexpected environmental conditions occurring. The mismatch is not only contributed to by the cognitive system but also by the environment, and not a result of a single event but of a complex (non-serial) web of events. To prevent accidents, the mismatch needs to be reduced and/or blocked.

Figure 4.4: The attributed causes of systemic accident models

Scope – a joint system and its environment

The scope of systemic accident models is larger than for sequential accident models but smaller than for epidemiological accident models. The scope varies with the selection of which parts are to form a joint system, and the parts selected
depend on the purpose of study. If the purpose is to understand the interaction between a driver and a device, then the joint system is the driver and the device is the environment. If the purpose is to understand the interaction between a driver using a device in the vehicle, then the driver and the device will form the joint system, and the vehicle will be the environment which the system interacts with.

**Accident evolution – an unexpected event combination in a network**

Accident process is a complex and interconnected web. What accident process is looked for in systemic accident model is no longer the evolution of events but the combination of events. The combination of events is the way they connected.

**Relation between causality and inferred causality – not equal concepts**

The inferred causes in systemic accident models differ from causes inferred in sequential or epidemiological models. The events or causes which bring about an accident in systemic models are coexistent in time (the unexpected combination of events), but need not have causal relations in the traditional sense as in the domino effect. As shown in Figure 4.5, there are a number of possible ways to have accidents.

---

**Figure 4.5: The accident causality of systemic accident models**

**Accident precaution – support the joint system stay in control**

Systemic accident models looks for a combination of events, and the preventive strategy is to try to remove all possibilities for a similar combination. If only one of the contributing events is treated, the accident possibility will temporarily be reduced, but sooner or latter new similar events will develop. This will result either in similar types of accidents, or new kinds of accidents if there exists another system whose events are partly shared with the current system. 

Prevention
therefore involves careful thinking about the connected events. From a system management view, if the accident system is a subsystem in some sense, then systems outside the current one also need to be taken into account.

### 4.3 The Evolution of Road Safety Paradigms

An OECD report (OECD, 1997) distinguished between four road safety paradigms which have been developed in the course of the twentieth century (see Table 4.1). The distinctions between the paradigms highlight existing differences of view in dealing with road safety. A short summary of these four paradigms is as below:

- The description of the first paradigm is described as *control of motorized carriages* in which the ideal of road safety is to control the use of vehicles (motorized carriages) in the same way as horse drawn carriages. The concept and countermeasures of road safety were mainly based on what had been learned from dealing with the safety of horse drawn carriages. The period involved a lot of tuning up of vehicle and driver, as well as regulations. The research of road safety was focused on “what” mechanical component needed to be engineered in short term countermeasures and “what” regulation needed to be initiated in long term countermeasures. The “what” question was addressed by studying statistic data of road accidents.

- The second paradigm is described as *mastering traffic situations* in which the focus was shifted from vehicle mechanics to drivers. At this period mechanical systems (i.e. vehicles) had been developed into a rather reliable and complex state, compared to their predecessors. The concepts and countermeasures of road safety were mainly based on knowledge gained from tuning of mechanical systems. “Driver errors” became the target of road safety. Researches aimed to answer “why” drivers commit errors. Researches were from multiple disciplines and answered the “why” question from their domain knowledge. Road accident countermeasures consequently were generated based on problem descriptions from different areas (e.g. vehicle, road infrastructure, driver) and disciplines (e.g. engineering, medicine, psychology, sociology).

- The description of the third paradigm is *managing traffic systems*. During the previous period a great number of concepts and countermeasures addressing “driver errors” had been developed. In this period the main problem became “how” to prioritize between these concepts and
countermeasures. Accident prevention therefore developed from separate accident prevention projects into a systematic road safety management. The main vision was to remove risks from the road system, especially the risks of injury.

Table 4.1: Development of road safety paradigms (Abstracted from OECD, 1997)

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Paradigm I</th>
<th>Paradigm II</th>
<th>Paradigm III</th>
<th>Paradigm IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decennia of dominating position</td>
<td>1900-1925/35</td>
<td>1925/35-1965/70</td>
<td>1965/70-1980/85</td>
<td>1980/85-</td>
</tr>
<tr>
<td>Description</td>
<td>Control of motorized carriage</td>
<td>Mastering traffic situations</td>
<td>Managing traffic system</td>
<td>Managing transport system</td>
</tr>
<tr>
<td>Main idea and focus</td>
<td>Use cars as horse drawn carriages</td>
<td>Adapt people to manage traffic situations</td>
<td>Eliminate risk factors from road traffic system</td>
<td>Consider exposure of risk, regulate transport</td>
</tr>
<tr>
<td>Main disciplines involved</td>
<td>Law enforcement</td>
<td>Car and road engineering, psychology</td>
<td>Traffic engineering, traffic medicine, advanced statistics</td>
<td>Advanced technology, system analysis, sociology, communication</td>
</tr>
<tr>
<td>Term used about unwanted events</td>
<td>Collision</td>
<td>Accident</td>
<td>Crash, casualty</td>
<td>Costs, suffering</td>
</tr>
<tr>
<td>Ideas concerning unsafety</td>
<td>Transitional problem, passing stage of maladjustment</td>
<td>Individual problem, inadequate morale and skill</td>
<td>Defective traffic system</td>
<td>Risk exposure</td>
</tr>
<tr>
<td>Data ideals in research</td>
<td>Basic statistics, answers on “What”</td>
<td>Causes of accidents, answer on “Why”</td>
<td>Cost/benefit ratio of means, answer on “How”</td>
<td>Multidimensional</td>
</tr>
<tr>
<td>Typical countermeasures</td>
<td>Vehicle requirement and inspection, school patrols</td>
<td>The three E’s doctrine, screening of accident prone drivers</td>
<td>Combined samples of measures for diminishing risks</td>
<td>Networking and pricing the transport costs</td>
</tr>
<tr>
<td>Effects</td>
<td>Gradual increase in both traffic and health risks</td>
<td>Rapid increase of health risk with decreasing traffic risk</td>
<td>Successive cycles of decrease of health and traffic risks</td>
<td>Continuous reduction of serious road accidents</td>
</tr>
</tbody>
</table>
The description of the fourth paradigm is *managing transportation systems*. The scope of road safety has been extended for each consecutive period. In this fourth period the scope is extended to encompass the framework of transportation as a whole. The concept for accident prevention in this period is not only reducing the risk of injury but also proactively minimizing the risk exposure. Accident prevention countermeasures address how to direct traffic into less risky modes and road sections.

The four paradigms illustrate an overview of how the road safety targets have evolved. The development has mainly been practical in nature and a community learning process (OECD, 1997). The earlier paradigms were not completely replaced by the later paradigms but the latter paradigms were built on the earlier paradigms. The community learning process showed an evolution in the accident prevention approach as well as an underlying accident model. Accident prevention has evolved from problem identification via cause identification and countermeasure generation to the prioritisation of countermeasures.

The underlying accident models have followed this development. The first and second paradigms, with their focus on mechanical and driver failures respectively, were shaped by underlying sequential accident models. Epidemiological accident models were introduced when the scope of accident prevention was extended to consider the whole road system, i.e. in the time of the third paradigm. In the period of the fourth paradigm, the accident prevention scope has extended to cover the whole transportation system, but accident prevention is still based on sequential accident models at the lower levels of accident prevention (company and management), and epidemiological accident models at higher level of accident prevention (government and regulators). This separation of hierarchical levels in the risk management of a socio-technical system is the main problem of accident prevention (Rasmussen and Svedung, 2000).

### 4.4 The Underlying Accident Model of Current Road Safety

#### 4.4.1 Driver errors as a main cause

In road safety two similar major studies were carried out in the 1970s’, one in the United States and in the United Kingdoms. The US study was performed by Indiana University and is described in Treat et al. (1977). The British study was performed by the Transport and Road Research Laboratory and is described in Sabey and Taylor (1980). In the both studies a multi-disciplinary expert team
conducted detailed post-crash examination of crashes satisfying predefined selection criteria. The crash site and the vehicle involved were examined for physical evidence and participants in the crash were interviewed in depth.

Base on such information, the main factors contributing to the crashes were identified (Evans, 1991). Results from the two studies are quite consistent, saying that road user factors are the sole contributing factors in 65% of all crashes in the British study and 57% in the US study and sole and/or contributory factors is 95% in the UK study and 94% in the US study. Only 5% of the crashes are linked to non-road-users factors (i.e. vehicle and road environment factors) in the UK study and 6% in the US study.

In short, for both studies the attributed causes in road accidents are road-user, vehicle and road factors, and among them road-user factors are far more often attributed than the other two. A similar conclusion was also made by Evans (1987), though he reduced the attributed causes to human and engineering factors.

Although driver factors were identified as the main causal factors in the 1970s studies, the categorization of driver factors was too general in their taxonomies. The development of road safety measures demands a detailed taxonomy of driver errors, and the taxonomy varies depending on the purpose of the analysis. For example, Tijerina (1996) proposed one taxonomy of crash contributing factors to aid in the development of crash avoidance system technologies, and Wierwille et al. (2002) proposed another taxonomy of driver errors for the development of infrastructure-related safety measures.

### 4.4.2 Linear accident process

The process of road accidents is usually described in terms of linear events. As one of the introductory examples shown, first the driver failed to shift the gear down resulting in the speed of the vehicle increasing, making the driver apply the hydraulic break which eventually failed, and thus the driver was no longer able to control the vehicle. Finally the vehicle struck road users and a vehicle at an intersection.

**Identical causality and inferred causality but opposite in direction**

The identified accident process which explains the occurrence of the accident is usually used “directly” in the selection of countermeasures. For example, the intersection accident, using the same example, can be avoided by either securing
that gear downshift always is successful, that the speed of the vehicle cannot increase in certain situations, or that the hydraulic break cannot break. It implies that other steep and long downgrade accidents in the future will follow the same process as previously identified.

4.4.3 Safety measures - eliminating or mitigating “driver errors”

The Triple E strategy (Gunnarsson, 1996), which was established perhaps as early as the 1930s, is broadly used in road safety. The Triple E stands for: Engineering, measures enacted in vehicle, road and traffic engineering; Education, training of drivers and traffic education in schools; Enforcement, ensuring and imposing obedience to traffic laws and regulations. Using the example of the rear-end accident: to avoid rear-end accidents, engineering measures as suggested by NTSB (2006b) can be the installation of collision warning systems on all new commercial vehicles and the installation of electronic toll collection systems on all toll plazas. Education measures are to teach drivers how to be prepared for queues before toll plazas. The Triple E strategy is a “driver errors” focused strategy. Enforcement and education are no doubt driver errors focused, and even though the engineering part could focus on vehicle and road, it still targets drivers’ errors.

4.5 Summary

Accident models are used in accident prevention to guide the search for causes and the prediction of effects. Accident prevention based on sequential accident models regards the accident process as a chain of events caused by operator or machine failures, and the aim is to improve the reliability of weak components. Accident prevention based on epidemiological accident models regard the occurrence of accident as a result of missing or weakened barriers, and the preventive aim is to install and strengthen barriers. Accident prevention based on systemic accident model regards the occurrence of accidents as results of a system loosing control, and focus is on helping the system stay in control.
Table 4.2: The essential concepts of accident models

<table>
<thead>
<tr>
<th>Accident models</th>
<th>Principle of search</th>
<th>Principle of prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequential</td>
<td>Factors contributing to operator and/or machine failure</td>
<td>Improve component reliability</td>
</tr>
<tr>
<td>Epidemiological</td>
<td>Factors contributing to the miss and/or weakened barriers</td>
<td>Install and strengthen barriers</td>
</tr>
<tr>
<td>Systemic</td>
<td>Factors contributing to the loss of control</td>
<td>Support system remaining in control</td>
</tr>
</tbody>
</table>

Current road safety on the micro level is based on sequential accident models and aims to improve the reliability of driver, vehicle or road by identifying their failures. The capabilities of road safety measures based on such analysis are limited. It only works if all road accidents are component failure accidents, and as was discussed in Chapter 2, this is not a suitable view for complex and coupled dynamic systems such as road traffic.

On the macro level, the development of road safety has evolved from the management of driver performance via management of road traffic system performance to the management of transportation performance. On this level, road safety is at present considered a management problem. This management approach leads road safety to a focus on selected and simplified problems, in the sense that they only address one level of the traffic systems, and therefore only will have local (sub-optimal) effects. This is also a consequence of using a sequential accident model.
5 APPROACHES TO ACCIDENT PREVENTION

Before the final discussion in Chapter 6 of the possibilities and benefits of pushing the accident modelling of road safety in a more systemic direction, the second question posed in the introduction needs to be addressed. Since the mission of accident prevention is to prevent accidents in the future, its focus should theoretically be on how accidents will happen rather than on how they did happen. Despite this, road safety has traditionally put much more emphasis on accident investigation than accident prediction, compared to areas such as nuclear power plant and chemical industries.

The underlying reason for this is most likely connected to the frequency of accidents. In Sweden, 18,029 road traffic accidents involving personal injury were reported by the police in 2004 (SIKA, 2005). That makes about fifty accidents per day or two accidents per hour. Extrapolating this into a global perspective, road accidents probably occur every second or so. As opposed to this, in nuclear power plants and chemical industries, there is just a few numbers of accidents per year, so there are actually very few accidents to investigate in comparison.

However, having many accidents to investigate does not automatically mean that this should be the main research activity. Instead it raises the question of whether road traffic safety should move resources from investigations of the past to predictions of the future, to accomplish better prevention measures. In this chapter, the two main prevention approaches, i.e. the passive and the proactive approach, are described and discussed, along with the analysis types (retrospective and prospective) used in each approach. It is concluded that the approach used will be determined by the accident model that underlie the analysis. Work based on sequential models needs only the passive approach, whereas work based on systemic models need both retrospective and prospective analysis. Therefore,
the end of the chapter an integrated approach using both retrospective and prospective analysis is described.

As pointed out by Heinrich et al. (1980), accident prevention is a cyclic process in which decisions are made in order to maintain or improve the performance of a system. The cyclic process contains a goal, a difference between the goal and the present safety state, an action to implement and a monitoring phase in which the results of the action are studied. This can be seen as a closed-loop control process (see Figure 2.3). The purpose of the control process is to achieve a desired safety level, e.g. an acceptable number of annual fatalities. In the cyclic process, safety management creates a construct, or an understanding of the systems present state, based on system feedback collected through for example system monitoring and data analysis. Based on the construct, an action is determined, which in accident prevention means remedies are selected and applied. Then the effects of the remedies are studied through the feedback from the system, a new construct is created, and the cycle is repeating.

![Figure 5.1: Accident prevention can be seen as a close-loop control process](image)

In a closed-loop control process, the control system can produce actions passively or proactively. The current system state is determined from the monitoring of the system. In the case of road safety, annual number of injuries and fatalities is a type of feedback. In order to produce an action to minimize the difference between actual numbers and what was aimed for, the construct describing the system needs to include reasons for the difference. Based on the construct of these reasons of
the difference, an action is produced. The produced action together with other actions will modify the state of the system.

In a passive closed-loop control process, an action is produced to reduce the difference between current and desired system state. In a proactive closed-loop control process, an action is produced not only to minimize the difference between current and desired system state, but also to minimize the difference between upcoming and desired system states. As a consequence, the produced actions will not always be the best actions for the current system state. Instead they will be a trade-off between the needs of the current and upcoming system states. Use of such feedforward control can reduce the efforts needed in pure feedback based control, especially in a dynamic environment where planning ahead really can give you an edge.

### 5.1 Passive accident prevention approach

A common approach of accident prevention used in practice is to patch the hole the sheep escaped through after it has run away, also called the Fly-Fix-Fly approach in air safety (Leveson, 1995). An escaped sheep is not purely a loss, since it tells us (at least) a hole existed and if luck where the hole is. Once the hole is identified and patched, sheep cannot escape from the same hole again. Ideally, there would come an end to all patching when all possible holes are detected and patched, i.e. all possible accidents have happened and been addressed. Unfortunately, this is only possible if the system remains completely unchanged, and very few systems are of that nature (road traffic certainly is not one of them). A continuous finding and patching of new holes is therefore the normal practical contents of accident prevention.
Figure 5.2: Passive accident prevention approach

If other holes are produced while some holes are patched, the target of the control system will shift toward keeping the total number of escaped sheep below an acceptable level. It then becomes an issue to decide in which order the holes should be patched in order to keep the numbers down. In the case of road safety, remedies or countermeasures are sometimes immediately developed if there have been one or two particularly serious accidents. In most cases however, remedies are produced only when a larger number of similar accidents have occurred.

Figure 5.3: A passive accident prevention approach chases after accidents
5.2 Proactive accident prevention approach

Taking the same example of patching hole, proactive accident prevention works somewhat differently compared to the passive approach. It is not about patching holes when the sheep are gone, it is about predicting where holes probably will occur and deal with them before any sheep escape in the first place. The action taken does not have to be a patch, i.e. a reinforcement of the existing fence. It may just as well be a decision to change fencing material overall, or shorten the renewal interval for fence posts. As discussed above, the action may not solve the immediate problems, but may be the better solution if also taking future problems into account. It is also a reflection of short-term and long-term safety management considerations in Heinrich et al.’s accident prevention model.

Figure 5.4: Proactive accident prevention approach

A proactive accident prevention approach contains both feedback and feedforward loops. The feedback loop informs the control system about the difference between current and desired system state. The feedforward loop informs the control system about the difference between upcoming states and the desired system state. The final remedies are often a compromise between what can be done and what should be done if time and resources were unlimited. The decision on final remedies depends on the seriousness of the current and predicted future problems.
5.3 Retrospective Analysis

The feedback loop discussed in the previous section can be referred to retrospective analyses done in practice. The purpose of retrospective analysis is to identify the contributing factors of an accident and address them with countermeasures. Below is a definition of retrospective analysis made by Cacciabue (2004):

*Retrospective analyses consist of the assessment of events involving human-machine interaction, such as accidents, incidents, or “near-misses”, with the objective of a detailed search for the fundamental reasons, facts, and causes (“root cause”) that fostered them.*

This is true regardless of which accident model the retrospective analysis is based on. For this discussion, a systemic accident model is chosen, to illustrate how it principally may work in practice.

Based on systemic accident models the occurrence of an accident is due to a mismatch between the performance of a joint system and the environmental conditions. Hence a retrospective analysis aims to find out why the performance of the joint system was unable to perform according to the demands of the environmental conditions and vice versa, i.e. why the environmental conditions demanded a level of performance which the joint system was unable to deliver.
For a detailed description about the application of the concept of joint cognitive system on road traffic see Hollnagel et al. (2003).

The results of a retrospective analysis are normally used to generate ideas for countermeasures, i.e. ways to reduce the mismatch between actual and demanded performance. There are three ways to do this. If the difference between the performance of the joint system and the demands from the environment is small and the joint system has spare capability, a situational increase in the performance of the joint system by using the spare capability can keep a mismatch from occurring.

If the difference between performance of the joint system and environmental demands is large and the joint system does not have spare capability, then the joint system must be given time and resources to prepare for the situation in advance, otherwise a mismatch will occur. To bring the performance of the joint system up to a specific level in this way usually requires a stretch of time and a series of actions. The time needed to prepare depend on several conditions, such as the difference between joint system performance and the environmental demands and the type of action(s) needed to reduce the difference. For details on the relation between time available and control of a joint system please see Hollnagel & Woods (2005).

The third way of reducing the mismatch is to focus on the environment rather than the joint system. It does not have to be the joint system which adapts, the environment can be made to adapt as well, i.e. by reducing the demands to a level which the joint system can handle. While a joint system normally can adjust quite rapidly, environmental conditions usually take much longer time to change. Adjustment of the environment therefore requires knowledge of upcoming mismatches much further in advance. The best solution to this problem is to be aware of possible mismatches already in the design phase for the environment. This approach is therefore more common on a safety management level where design decisions can be made, rather than have to be lived with, and in other design groups. Focused work on designing the environmental conditions so they stay within the performance boundary of a user or a joint system is actually the main principle of all user-centred design.
5.4 Prospective Analysis

The feedback loop discussed in the section 5.2 can be referred to the retrospective analyses done in practice. The proactive approach to accident prevention is about prediction of future problems or accidents. Cacciabue (2004) defined prospective analysis as below:

*Prospective analyses entail the prediction and evaluation of the consequences of human-machine interaction, given certain initiating events and boundary configurations of a system.*

Such predictions and evaluations are related with analysis techniques, e.g. hazard identification, hazard analysis, reliability analysis and risk analysis.

5.4.1 Hazard identification

To prevent accidents, system designers must know and control the states which precede the accident. Hazards are states that solely or in combination have the potential to do harm or which can lead to accidents, e.g. an over-loaded truck and/or a long downgrade. A few techniques for identifying hazards have been developed, e.g., HAZOP, FMEA. These techniques are essentially structural ways to stimulate a group of experts to apply their personal knowledge to the task of identifying hazards. Since not all hazards are equally important, identified hazards are ranked according to their effect and likelihood, qualitatively or quantitatively. Which hazards are further analysed depends on their effect on accidents and the goal and resources of a safety study. Knowing hazards alone is however not sufficient to prevent accidents effectively. At most, measures can be passively applied to constraint the effects of the hazards, e.g. load inspections or rumple strips. In order to prevent the occurrence of hazards, their causes and the way they develop must be analysed.

5.4.2 Hazard analysis

The purpose of hazard analyses is to find causes of accidents. Hazard analyses can be done deductively and inductively. Deductive hazard analyses start from hazards and trace backward through links of undesired events to find causal factors. A typical deductive analysis technique is Fault Tree Analysis (FTA). Inductive hazard analyses on the contrary starts from a failure mode of a physical part or a human and searches forward through events to find probable consequences. Event Tree Analysis (ETA) is a typical example of the inductive analysis technique.
Safety analysis can be done qualitatively, as in the steps of risk analysis described later, or quantitatively. Quantitative risk analyses can be seen as the extension of qualitative risk analysis. Quantitative risk analyses helps researchers prioritize by providing exact assessments of hazard severity and likelihood, or risk levels. Usually the activity is done by creating a quantitative risk matrix. A line is drawn in the matrix representing an arbitrary breakpoint called the protection level. Hazard control efforts are then concentrated on the hazards above the desired protection level.

### 5.4.3 Risk analysis

Risk is a frequently used term with a vague definition. According to the Webster Dictionary, risk as a noun can refer to “someone or something that creates or suggest a hazard” or the “possibility of loss or injury”. Both these definitions are required in risk analysis.

The first definition of risk refers to that which can create hazards. A hazard is a state which may promote an activity developing into an undesirable event. For example, a construction vehicle left on a closed runway is a hazard, as seen in the airplane accident in the introduction. Although according to the definition of Webster Dictionary, hazards are created by humans or machines, hazards in fact also can come from nature. For example, darkness, fog and rain can facilitated the collision of the airplane taking off with the construction vehicle on the runway.

The second definition of risk represents a mathematical representation of the level of safety of a system which is performing an activity under specific conditions. Since there are several possible consequences with different degree of loss, the number will refer to an average loss of the system. The risk for a system is calculated by mathematically averaging its possible losses, i.e. the sum of the products of the probabilities for, and losses created by, undesirable events. The risk assessed in risk analysis is objective risk, in contrast to subject risk that is assessed by a person when facing a certain situation.
5.4.4 Reliability analysis

The purpose of risk analysis is to estimate the risks of an activity. In a reliability analysis, the purpose is to point out what and where unreliable components are. Both reliability analysis and risk analysis are decision making tools. The results of a reliability analysis show the reliability of a system. Decisions can then be made by comparing actual reliability of the system with a desired level of reliability.

If actual reliability is less than the desired level, action is needed to improve the reliability of the system. If actual reliability is higher than desired reliability, there is no need to make any changes to the system. Also, by investigating the reliability of components and studying the relation between them, the results of a reliability analysis will show which component(s) need to be engineered and the reliability level it must meet. Reliability analysis has succeeded in improving the reliability of many systems.

A reliable system, if not completely reliable, may fail sometimes. If a system will fail sometimes, severity becomes an issue. The goal of safety is to improve the safety of a system rather the reliability of a system. With reliability based engineering, it is possible that if the reliability of a system is increased, the severity of a system failure may also increase, even though it occurs more seldom. Risk analysis based on reliability analysis must therefore takes the severity into account.

A complete risk analysis should contain both a qualitative and a quantitative risk analysis. If there is no need to compare the severity of risks or to know the exact risk levels of a system, a qualitative risk analysis is enough. Qualitative risk analysis is a must in any risk analysis and is prior to quantitative risk analysis.
5.5 Risk Analysis, Risk Assessment and Risk Management

The term risk analysis is used differently in the methods described above. In some of them, risk analysis refers to the whole process of risk identification, risk quantification and risk reduction, but in other methods it signifies only the first part. Terms like risk assessment and risk management are also used to describe risk analysis process. To avoid unnecessary ambiguity, this thesis refers to the definition used in the ISO standard (ISO/IEC, 1999):

- **Risk Analysis** consists of scope definition, hazard identification and risk estimation. The result of risk analysis is a risk model which describes the relation between an initiating event and its possible consequences together with a number of hazards.

- **Risk Assessment** includes risk analysis and risk evaluation. Risk evaluation compares different options. The result of risk evaluation is a list of options that fulfil the requirements of the set risk level(s). An example of a risk assessment consists of following steps (Kirchsteiger, 2002):
  
  Step 1: Hazard identification - Identification of sources with the potential to cause undesired outcomes to subjects of concern that is the focus of the estimation of likelihood.
  
  Step 2: Event scenario assessment - Identification of the initiators and sequences of events that can lead to the realisation of the hazard.
  
  Step 3: Consequence assessment - Identification and assessment of the consequences of the realised hazard.
  
  Step 4: Risk Characterisation - This step consists of two parts:
  
  Step 4a: Risk estimation - Assessing and expressing the likelihood of the consequences and describing the quality of such estimates.
  
  Step 4b: Risk comparison - Comparing derived risk estimates to specified guidelines/criteria/goals and describing the dependence of theses estimates on explicitly specified assumptions.
  
  Step 5: Decision making - Deciding on actions to take based on the risk evaluation.

- **Risk Management** consists of risk assessment, risk reduction and monitoring. If the results of risk assessment show the system under study to be below the acceptable risk level and there is nothing to be gained by modifications (e.g. lower risk level, lower costs, less human resources),
there is no need to make any modification of the system. Otherwise, one of the action options will be chosen and the risk of the modified system will be assessed and monitored. The process is iterative.

Changes made on system can be planned or unplanned. A planned change is an intentional alteration of the system, such as the introduction of Adaptive Cruise Control (ACC). With planned changes, the possible effect of the planned change on system risk can be assessed and risk reduction action can be taken if the new risk level is above the acceptable level. An unplanned change is an unintentional alteration of the system, such as the increasing use of mobile phones in vehicles.
The risk management can be also compared to a control process. Risk analysis provides a controlling system, e.g. the road administration authority, a construct of current safety situations, e.g. risk level, risk factors. The controlling system bases on the construct and other information, e.g. the possible change in the controlled system, determines an action. The action is applied on the controlled system, e.g. installation of warning signs before steep downgrade. Then another risk analysis is conducted and the process will be repeated again.
5.6 Risk Analysis Methods in Road Safety

Several risk analysis methods have been developed in road safety. In this section, a review of five risk analysis methods is made. The methods are all used in road transport. The methods developed in ADVISORS (ADVISORS, 2001) and RESPONSE2 (RESPONSE2, 2005) were developed for assessing the risk of advanced driver assistance systems. These methods contain analysis techniques for analysing technical and human failures. The method proposed in ISA (Jagtman et al., 2005) is for controlling hazards in intelligent speed adaptation systems. FICA (Ljung et al., 2004) developed a method for accident and incident analysis leading to new road safety measures. Lastly there is the Traffic Conflict Technique (TCT; Hydén, 1987). The last three methods only concentrate on human reliability analysis. Following the description above, these projects can be described according to the techniques they use for hazard identification and hazard analysis of technical and human failures. The techniques are listed in the table below and briefly described in following sections.

Table 5.1: Traffic safety analysis methods

<table>
<thead>
<tr>
<th></th>
<th>ADVISORS</th>
<th>RESPONSE2</th>
<th>ISA</th>
<th>FICA</th>
<th>TCT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard Identification</td>
<td>Technical failure</td>
<td>Human failure</td>
<td>Technical failure</td>
<td>Human failure</td>
<td>Human failure</td>
</tr>
<tr>
<td>Hazard Analysis</td>
<td>FMEA</td>
<td>FTA</td>
<td>FMEA</td>
<td>Human HAZOP</td>
<td>DREAM</td>
</tr>
<tr>
<td></td>
<td>SLIM</td>
<td></td>
<td></td>
<td>Traffic Conflict Study</td>
<td></td>
</tr>
</tbody>
</table>

5.6.1 FMEA and Human FMEA

Failure Modes and Effects Analysis (FMEA), as used in ADVISORS and RESPONSE 2, uses a prospective search for consequences starting from initiating failures of individual components, following an underlying sequential accident model. The first step in an FMEA is to identify and list all components and their failure modes. For each failure mode, the effects on all other system components are determined along with the effect on the overall system. Then probabilities and consequence severities for each failure mode are calculated.

The Human FMEA used in RESPONSE 2 is similar to regular FMEA but concentrates on human failures. The details about how probability and severity of human failure modes are calculated are however not described in the project.
5.6.2 FTA

Fault Tree Analysis (FTA), used for analysing human failures in ADVISORS, uses a backward search starting from top events to the causes of the top events. The top event is a possible (unwanted) outcome, e.g., a collision of two cars. FTA uses Boolean logic to represent the combinations of possible events that can constitute a top event. The search produces a tree of events rather than a single sequence.

5.6.3 SLIM

Success Likelihood Index Method (SLIM), also was adopted in ADVISORS, assesses the operator reliability by referring to a scenario and its Performance Shaping Factors (PSFs). Each PSF is rated and its relation to the others is assessed. The sum of the weights is multiplied by the rating for each item to derive the Success Likelihood Index (SLI). The SLI indicates the relative likelihood of different errors. The SLI is transformed to a probability value by selecting anchor values and using a calibration equation.

5.6.4 Traffic HAZOP

As their name implies, Traffic HAZOP (Jagtman et al., 2005) bases on Hazards and Operability Analysis (HAZOP). HAZOP is designed to find every conceivable process deviation, and then look backwards at possible cause and forwards at possible consequence linearly. The approach is based on stimulating creativity and imagination through a structured brainstorm, in order to think of all possible manners in which hazards and operability problems can occur. Because HAZOP analyses needs well-described processes, they usually are applied quite late in the design process.

5.6.5 DREAM

Driver Reliability and Error Analysis Method (DREAM; Ljung, 2002) is an accident analysis method used in the FICA project, but can be used in risk analysis. A DREAM analysis starts from identifying possible error modes of a system and stop when possible MTO factors are identified. The method assumes that there are limited types of error modes. They represent the possible ways for a system dysfunctional behaviour to manifest itself in the dimensions of time, space and energy. The possible error modes are illustrated in the following Table.
Table 5.2: The error modes of DREAM

<table>
<thead>
<tr>
<th>General effects</th>
<th>Specific effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timing</td>
<td>Too early / Too late / Omission</td>
</tr>
<tr>
<td>Duration</td>
<td>Too long / Too short</td>
</tr>
<tr>
<td>Force</td>
<td>Too little / Too much</td>
</tr>
<tr>
<td>Distance</td>
<td>Too far / Too short</td>
</tr>
<tr>
<td>Speed</td>
<td>Too fast / Too slow</td>
</tr>
<tr>
<td>Direction</td>
<td>Wrong direction / Wrong movement type</td>
</tr>
<tr>
<td>Object</td>
<td>Neighbour / Similar object / Unrelated object</td>
</tr>
<tr>
<td>Sequence</td>
<td>Reversal / Repetition / Jump forward / Wrong action</td>
</tr>
<tr>
<td>Quantity/volume</td>
<td>Too little / Too much</td>
</tr>
</tbody>
</table>

Risk analysis in DREAM is done by iterative searches of consequents from their antecedents. The links of consequents and antecedents are described in link tables. A consequent usually has more than one probable antecedent. The selection of antecedents is assisted by referring to a context description. The analysis completes when all data collected from the accident or incident investigation is accounted for. The analysis produces a tree of events as in FTA, but the process of structuring the tree is dynamic and non-hierarchical, which makes it quite different from FTA.

5.6.6 Traffic Conflict Technique

The Traffic Conflict Technique is seen as a risk analysis technique for a selected road section in this thesis. Traditionally, the road sections selected to be studied are the sections which has been identified as a high accident rate road section (HARRS). A conflict is a near-incident situation which is seen as a precursor of accidents. By studying conflicts on a selected road section, the conflict technique is able to assess the risk level of the road section and identify both possible causes of the risk as well as suitable countermeasures to reduce the risk. The causes of conflicts normally attributed are inadequate driver behaviours, which sometimes are enhanced by unfriendly road and vehicle design. Countermeasures are focused on road infrastructure modification. The underlying accident model of conflict techniques is the sequential accident model. Conflict techniques are both risk identification and assessment methods.
5.7 Integrated Retrospective and Prospective Analysis

When doing accident analysis and prevention in practice, the researcher(s) rarely use just one of the retrospective and prospective analyses. The retrospective and prospective analyses can actually be seen as the endpoints of a methodological scale, where everyday work normally will include both types of analysis. The difference between domains will be in how efforts are shared between the two. In a domain where the consequences of a single accident may be catastrophic on a large scale, such as with nuclear power plants, focus is normally put on both retrospective and prospective analyses, but with a bias toward the proactive approach. In domains where each accident has relatively limited consequences, such as car crashes, focus is normally on a retrospective analysis, i.e. a bias toward the passive approach.

So in reality, most teams work with a combination of retrospective and prospective analysis, even in a passive approach. The concept of integrated retrospective and prospective analysis emphasizes that a comparable balance should be made between retrospective and prospective analyses. Approaches which lean solely on either retrospective or prospective analysis are inadequate. For example, over-emphasis on retrospective analyses reduces the capability to foresee probable accidents and slows responses. Over-emphasis on prospective analyses is more inadequate than over-emphasis on retrospective because there is no ground to base it on.

Cacciabue (2004) proposed a methodology, called Human Error Risk Management for Engineering Systems (HERMES), aimed towards ensuring the safety of socio-technical systems. The main ideal of the HERMES methodology is to integrate prospective and retrospective analyses into a logical analytical process. In the integrated analysis method, the results of both analyses can support each other, so the analyses combined can generate better measures than they do separately.

The HERMES methodology emphasizes the following concepts:

- Both prospective and retrospective analyses must rest on a common empirical and theoretical platform, hence
- The results of retrospective analyses can support the conduction of prospective analyses, and
The results of prospective analyses can refine the results of retrospective analyses.

Any proactive accident prevention approach should be based on concepts similar to the concepts of the HERMES methodology. The HERMES methodology emphasizes the importance of a common theoretical and empirical platform for both retrospective and prospective analyses. The theoretical platform refers to human factors theories and models of Human-Machine-Interaction (HMI) which describe the function of a human-machine system, e.g. a human information processing model (Wickens, 1992) and joint cognitive systems (Hollnagel, 2004). The empirical platform refers to the context where an HMI is implemented. These contextual conditions are important for making sense of, as well as predicting the behaviour of, a cognitive system in both retrospective and prospective analyses.
6 DISCUSSION AND CONCLUSIONS

In the thesis so far, the theoretical state of traditional accident prevention in road safety as well as the theoretical developments in other safety related areas have been described (Chapter 2). Then the discussion in Chapter 3 showed that the developments in modern road traffic are pushing the whole system in a direction of increased complexity and dynamic coupling, with the conclusion that the current approach to road safety needs reviewing and probably replacement, in order to deal with these changes.

In the introduction it was stated that all safety work rests on an accident model, and to alter the approach to road safety, a replacement of the current accident model in use would therefore be a first step. In order to know what we are replacing, as well as what to replace it with, Chapter 4 described three general types of accident models. As the epidemiological models were found to use the same basic axioms as the sequential ones, those two were clustered together. That left us with two general types of accident models, i.e. sequential and systemic.

When looking at the work of current road safety, it was concluded that it rests on a sequential accident model, and as this is not suitable for complex systems, it needs to be replaced by a systemic model. This conclusion was further supported in Chapter 5 in the discussion of different approaches to accident prevention. There it was showed that sequential accident models promote a passive, retrospective approach to prevention, whereas systemic models promote a more integrated approach with a lean toward a proactive approach based on prospective analysis and prevention, and the latter is believed to be more useful in preventive work in complex systems.

The rest of Chapter 6 will be dedicated to spell out in more detail how the adoption of a systemic perspective affects four important areas of road safety, i.e.
road system modelling, driving modelling, how causes of accident and incidents are searched for and finally road safety strategies. These descriptions contain condensed versions of work which has been done in the FICA and the AIDE projects, which can be found in the appended papers.

6.1 Accident Modelling for Modern Road Traffic (ref paper I)

A prerequisite for studying a system is to have a model of the system (see also paper I). A model is an abstraction of the system under study. Abstraction means that some characteristics deemed less important are removed. Models provide a mean to explain known system behaviours and predict unknown system behaviours. The law of universal gravitation, for instance, explains both the encirclement of planets in the solar system and was used to discover at the time unknown distant planets Uranus, Neptune, and Pluto.

Approaches to road safety based on systemic or sequential accident models have the same goal, i.e. to achieve safe road traffic. However, they differ in the way they wish to achieve that goal. In the classical or traditional view, accidents are due to malfunctions or errors of components in a system, or combinations of malfunctions (event trees or fault trees). The system will be accident free if all errors are identified and controlled. As opposed to this, in the systemic view, accidents emerge from a combination of normal events, specifically from combinations of the normal variability of functions of parts and subsystems. Safe road traffic is therefore not achieved by eliminating errors, but by strengthening the dynamics which keep variability and deviation under control.

To put things very bluntly, the traditional road safety approach, with its basis in sequential accident models, can be said to have been dedicated to road “unsafety” research rather than road safety research (OECD, 1997), with accidents as the main concern. Traditional road “unsafety” research generally begins with accidents or accident situations and end up with remedies. From the study of accidents, one learns how accidents occur, what caused them, what remedies can prevent them and how well the remedies work. The traditional perspective thereby limits itself, by watching only the negative side of driving and road traffic system management. It looks for root causes, i.e. basic failures which explain the accident occurrences and try to fix the root causes. Traditional road safety has been very busy chasing from one accident to the other, fixing cause after cause. In analogy
with the human body, the focus has solely been on searching for diseases and curing them, or at least relieving the pain.

This perspective will not be sufficient when dealing with the modern road traffic environment that is emerging due to technological advancements and increased transportation needs. To quote Summala:

*It (the traffic system) is a system in which millions of cars move on streets and roads every day so that their driving paths cross each other and critical situations must arise due to pure random processes. Every day millions of cars meet other ones with a speed difference of 100 to more than 200 km/h, separated only by a few meters from each other, while the drivers' attentiveness, the steering system of the cars, the lateral slope of the road, with wind, and other factors result in a scatter of each car's lateral position. Accidentally, by a mere chance or as a result of a failed correction maneuver, a frontal collision occurs sometimes. Every day millions of cars enter curves in which slowing down is necessary, and the approach speed is again dependent on a host of factors, including varying estimates of the own speed, the curvature, and the pavement: due to this normal fluctuation of speeds, accidents will occur. Furthermore, the traffic system includes pedestrians and cyclists who show even more scatter in their behavior on the roads.*

So the very basis of traffic accidents consists of the random processes, of the fact that we have such a complicated traffic system with so many participants and so much kinetic energy involved. And when millions of drivers habitually drive at too short safety margins and do not make any allowances for (infrequent) deviant behavior or for (infrequent) coincidences, this very normal behavior results in accidents (cf. Summala, 1985).

If we instead of the traditional approach were to build road safety on a systemic accident model and perspective, things would be quite different. In contrast to road “unsafety” research, we would by definition start with a safe or normal driving situation, and the research focus would be on how the normal situation can be maintained under various conditions, especially when there is complex interaction between system(s) and environment. The systemic view aims to understand how components of a system work together to keep the system in control. In the case of an accident, the purpose of the analysis will be to figure out
why the system failed to remain in control rather than to look for which component to blame. By knowing why the system fails to remain in control in a specific situation, remedies are generated to strengthen the capability of the system to cope with the situation. Again comparing the road traffic system to a human body, a systemic view aims to maintain the health of the body, i.e. keeping it from getting sick in the first place. Systemic researches are dedicated to understand the interaction between organs and how they jointly keep the body in a healthy condition.

As an anecdote, it is interesting to compare the systemic method in system safety with Chinese medicine, since both are based on a systemic concept and aim to keep a system in a state of good function. Chinese medicine has been dedicated to understanding the interaction between organs and how they jointly keep the body in a healthy condition. In the case of sickness, the body (or organs together) is unable to deal with the environmental conditions, and one of the organs may suffer an abnormal condition, e.g. irritation. However, the irritated organ is a manifestation of the problem rather than its cause. The irritation may be due to an unbalance between several organs. To cure the disease it is necessary to treat the system as whole rather than just a specific organ, which normally makes the treatment take quite some time. However, once the patient is cured the system is in a stable state and the problem will not return. The golden rule of Chinese medicine is that regular doctors cure sickness but excellent doctors cure non-sickness. This rule also stresses the importance of preventing rather than curing diseases.

6.2 Driving Modelling

To understand the occurrence of road accidents, knowledge of how driving is performed is essential. A driving model is therefore an implicit but critical component of an accident model. There are two ways to model driving. The first and most accepted way is to model driving in terms of the interactions between sub-systems and components (a structural approach). Both sequential and epidemiological accident models model driving this way. Driving is described as a driver controlling the vehicle and interacting with the environment (Figure 3.2). Since drivers are regarded as the most problematic sub-system in the traffic system (Treat et al., 1977; Sabey & Taylor, 1980), the attentions of road safety have been spent on “driver errors”, with driving models there to explain the error making mechanism (e.g. Rumar, 1985).
Another type of driving model is to model driving in terms of its functions. The focus of a functional approach is on how functions are organized to achieve system goals rather than on the interactions between sub-systems and components. If the focus of road safety is going to switch to a systemic perspective, then a new view on driver modelling is needed as well. That view should preferably be based on system modelling in terms of functions, as this is an inherent trait of systemic models. The basics of such a view as well as two examples will be described in this section.

**6.2.1 Cognitive systems**

The functional approach, as opposed to the structural approach, provides a clear and simple alternative in the modelling of behaviours of complex systems. It treats the driver and the vehicle as a cognitive system. The behaviours of a cognitive system are goal oriented. From a control theory perspective, the behaviours aim to achieve a specific goal value or minimize the difference between the goal value and the current state. A system usually has more than one goal, e.g. being at the destination on time, having as short driving time as possible, avoiding collisions. The goals affect the ways in which the system organizes and adjusts its functions. In order to be at the destination on time for example, a driver may increase his average speed and some traffic checks may be skipped. The goal of having no accident may be overridden by the goal of being at the destination on time. Although the behaviours of a cognitive system are goal oriented, they also need to be adapted to local situations, e.g. visibility, road geometry, traffic flow. If the system does not adapt, it most likely will lose control.

A cognitive system is a system which is able to adapt itself to the change of environments so that its goals can be achieved (Hollnagel and Woods, 2005) or the mismatch between the goal and the status quo of the system can be minimized. A human being who can adapt his/her behaviours, e.g. higher cruising speed, to the changes of environments, e.g. better road infrastructure and vehicle performance, is definitely a cognitive system. Moreover, a human being (driver) and a machine (vehicle) is also a cognitive system, because the joint driver-vehicle system can adapt itself to the changes of environment. For the same reason, an intelligent machine is a cognitive system too. So as one or a group of operators and one or a number of non-intelligent and intelligent machines is a joint cognitive system.
The behaviours of cognitive systems does not always passively follow a planned procedures but very often proactively rearrange and skip some procedures so that specific goals and better performances can be achieved. The specific goals in driving are such as arriving at a destination on time, lower gas consumption, and performance goals are such as fewer standstills, fewer braking events, constant cruising speed.

6.2.2 Disturbances

Disturbances are events that are not included in the original plan. For instance, traffic jam always occurs on your daily route to the office. That traffic jam is not a disturbance because you know about it and take it into account when you plan the trip. An accident on your route to work on the other hand may be a disturbance, if you are not informed about it before arriving at the accident site. Disturbances do not need to be unexpected. We often expect something to happen, we just do not know exactly when and where it will. Since disturbances are not included in the original plan, they will lead to minor or major changes of the plan. Usually a limited time is available for the changes.

6.2.3 Examples of driving models based on a systemic perspective

Models of this sort, which are relevant for road safety, are the hierarchical control model (Michon, 1985) and the Driver-in-Control model (Hollnagel et al., 2003). Michon (1985) proposed his hierarchical control model for modelling the driver-vehicle system. He divided driving into three levels of control. At the Control level, very frequent and time limited events are dealt with, such as maintaining speed and following a route. Actions at the Control level are automatic. At the next level, the Manoeuvring level, frequent and time limited events are dealt with, such as overtaking or entering/exiting a roundabout. Actions at the Manoeuvring level are procedure-based. At the Strategic level, rare and less time constrained events are dealt with, such as routing, scheduling.

The Driver-in-Control model has a hierarchical control structure similar to Michon’s but is divided into four levels. The major difference between the two models is that the Driver-in-Control model describes control as a cyclic process ongoing at each of the four levels. The cyclic process emphasizes that control is not only passive but also proactive. Another major difference is that the Driver-in-Control model also clearly points out that the functions comes from a joint driver-vehicle system (cognitive system), while Michon’s do not. The concept of a
cognitive system is important in modelling the dynamics and complexity of socio-technical systems.

6.3 Causes of Road Accidents (ref papers II and III)

The major problem of sequential and epidemiological accident models in the analysis of complex systems is that they aim to identify causes which are individually made by a sub-system or component and are due to their internal failure(s). Systemic accident models, on the contrary, say that the causes of an accident cannot be attributed to individual sub-systems or components but rather to a group of them. The reason for this is that the interactions between sub-systems and components are so critical to the occurrence of accidents that they can not be neglected.

6.3.1 Complex interactions

Evans (1991) pointed out that many factors are associated with every traffic accident. A popular classification of accidental factors is Haddon’s matrix (Haddon, 1972). Haddon’s matrix is a two-dimensional 3 x 3 matrix. One dimension of the matrix contains the three elements human, vehicle/equipment, and environment, which are recognized as the contributing factors of accidents. Another dimension of the matrix consists of the three phases pre-crash, crash, and post-crash, representing the phases of accidents. In Haddon’s matrix an accident can be the result of several factors coming from different cells of the matrix. However, as Evans (1991) pointed out, there are complex interactions between these factors which the matrix does not account for. In other words, Haddon’s matrix is a sequential accident model of the epidemiological type which does not deal very with interactions. Evans says:

If drivers know that their vehicles are in poor safety condition, they may exercise increased caution. If a hazardous section of roadway is rebuilt to higher safety standards, it is likely that drivers will travel this section faster than before the improvement, or with less care.

If drivers know that their vehicles are in poor safety condition, they may exercise increased caution. If a hazardous section of roadway is rebuilt to higher safety standards, it is likely that drivers will travel this section faster than before the improvement, or with less care (Evans, 1991).
In other words, a change in one factor causes changes in related factors, and this may bounce back, i.e. the responsive changes in the related factors may cause a change of the original factor again, but these interactions become invisible when the system is studied at the level of sub-system or component. Take for example the driver’s failure to keep adequate speed in the interaction accident presented in the introduction. If the driver is studied alone, the result of the analysis probably will assign the failure to the driver and attribute the cause as inexperience or inadequate training. If the brake system is analyzed alone, the cause of the accident would be something like inadequate design or poor maintenance. Systemic accident models on the other hand stress the importance of the complex interactions between components. An analysis from that perspective would say that the whole system had deviated from a healthy state. The interaction between the company’s inadequate recruitment procedures, the mechanic’s misdiagnosis of the brakes and the lack of information on ASA adjustment is what made it possible for the accident to happen.

6.3.2 Deviation

Another point on which systemic accident models differentiate from sequential and epidemiological accident models is that the contributing factors in systemic models do not necessary have to be failures of some kind. The term failure always conveys the notion that a thing cannot provide its normal function, e.g. a faulty brake, a drunk driver. However, as can be seen in incident and accident analysis from a systemic perspective, most of the time the factors contributing to accidents and incidents consist of deviations from a normal state rather than complete failures. Things still work, they just do not work well enough to handle the situation, e.g. a rusty brake discs, a drowsy driver.

It is hindsight to classify a deviation as a failure. A deviation on function, e.g. late observation, usually does not cause accidents. Examples are found in the in-vehicle observations done in the FICA project. Three drivers reported that they observed were late in observing a vehicle catching up from the rear in the lane they were going to change to, at the same location of a rather complex highway exit system. Factors which contributed to the late observation are various, including unfamiliarity with the route, inadequate location of a direction sign, obscured vision due to the exit system design, and little time available due to high vehicle speeds. None of these deviations resulted in an accident however. For example, one novice driver did not abort the lane change manoeuvre even though
the catching up vehicle was dangerously close, but there was no accident none the less.

Since the geographic location of these incidents was common in our limited number of observations (three out of five), an inquiry into an accident database called STRADA, which contains all police reported traffic accidents in Sweden with geographic locations marked on a map, was made to determine accident frequency for that location in the past five years. The result was surprisingly out of expectation. There was no accident reported at that location. Based on available data and investigation of the location, a reasonable inference for this is that the catching up vehicles take action to avoid potential collisions, since the drivers in those vehicles have a clear view of the road and vehicles changing lanes ahead. In other words, the possible consequences of deviations in one joint driver-vehicle system are mitigated by increased system performance in another system (the system uses its spare capability to deal with the increased demands from the environment).

6.4 Road Safety Strategy (papers II and III)

Road safety strategies based on sequential and epidemiological accident models focus on the elimination and mitigation of sub-system or component failures. The shift from the traditional accident models to systemic accident models concurrently must lead to a change in road safety strategies, going from patching to tuning.

6.4.1 System turning and accident prevention

Accident prevention from a systemic point of view is simply stated to tune a system so that the probable accidents of the future will not occur. The term system in a systemic accident model refers to a socio-technical system, i.e. something which contains at least a human and a machine. To prevent probable accidents means to tune a socio-technical system so that mismatches are unlikely to occur. To know what in a socio-technical system need to be tuned and how they should be tuned are key tasks in accident prevention.

The occurrence of an accident can be seen as the performance of a socio-technical system being unable to meet the demands of an environment, with negative consequences for the system or environment as a result. For example, in a steep downgrade, a truck must counter the acceleration produced by gravitation so an
appropriate speed can be kept. The mismatch between the acceleration induced due to the road slope and and the deceleration capabilities of the truck make the truck go too fast. However, the production of deceleration is not by the truck alone, but also by the actions of the driver and the surface condition of the road, and the acceleration is only produced only by the downgrade but also by the overloading of the truck.

Although the concept of mismatch is also adopted in Task-Capability Interface Model (Fuller, 2000), that model regards the occurrence of road accidents as the performance of a driver being unable to meet the demands of an environment. As the example above show, the driver is obviously not the only one contributing to the mismatch, the environment does its fair share as well. The mismatch is therefore a result of complex interactions between several factors in both system and environment.

6.4.2 Minimize mismatch

Since the occurrence of accidents is due to the mismatch between the performance of a Joint Driver-Vehicle-Road System (JDVRS) and the demands of an environment in systemic accident models, there are three reasonable ways to minimize the mismatch: either by improving the performance of JDVRS, reducing the demand of an environment, or both. A JDVRS is a system which consists of a driver, a vehicle and a stretch of road. There is no absolute answer to the question of which road accident prevention should take, but a rule of thumb taken from the Law of Requisite Variety (Ashby, 1956) in Cybernetics might be useful.

\[
\text{Min} \ (V_O) = V_D - V_R
\]

Figure 6.1: The law of requisite variety
... If the varieties are measured logarithmically (as is almost always convenient), and if the same conditions hold, then the theorem takes a very simple form. Let $V_D$ be the variety of $D$, $V_R$ that of $R$, and $V_O$ that of the outcome (all measured logarithmically).

$D$ represents a dynamic system, $R$ is the controller of the system, and $O$ is the outcomes of the system. So that

... If $V_D$ is given and fixed, $V_D - V_R$ can be lessened only by a corresponding increase in $V_R$. Thus the variety in the outcomes, if minimal, can be decreased further only by a corresponding increase in that of $R$.

This is the Law of Requisite Variety. The point of the law is that to keep a system under control the variety of the controller must at least be as large as the variety of the process to be controlled. As Ashby stressed:

... only variety in $R$ can force down the variety due to $D$; variety can destroy variety.

A mismatch can therefore be overcome either by increasing the variety of the controller or by limiting the variety of the process. Therefore, the rule of thumb in accident prevention is to increase the variety of the JDVRS to the same level as the environment or to reduce the environment variety to that of the JDVRS.

### 6.4.3 Reduced mismatch through JDVRS support

On way of reducing accidents is to support the performance of a JDVRS so it can meet the demands of an environment. The support concept is to amplify the capability of the JDVRS, i.e. the capability of JDVRS is below the demand of an environment if there is no support. There are a number of such supporting devices which already are, or will be, used in road traffic.

Traditional examples are anti-lock braking system (ABS) and direction signs. ABS supports the JDVRS in having sufficient deceleration force by avoiding locked wheels when braking. Appropriate design and location of direction signs help drivers navigate complex road systems toward their destinations. A number of more recent supporting systems are shown in Table 6.1.
Table 6.1: Examples of systems designed to support a JDVRS

<table>
<thead>
<tr>
<th>Function</th>
<th>System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigation</td>
<td>Route navigation system</td>
<td>The system enables a driver to enter a destination, the system then computes the best route for the driver to follow. The system uses GPS position measurement of the vehicle together with a digital map.</td>
</tr>
<tr>
<td>Lateral control</td>
<td>Lane keeping</td>
<td>Supports the drivers' lane following task. If a deviation from the expected vehicle trajectory along a lane is detected, the system steers the vehicle back to the centre of the lane applying an appropriate steering wheel force in the appropriate steering direction.</td>
</tr>
<tr>
<td></td>
<td>Blind spot monitoring</td>
<td>The blind spot are the lateral areas of a vehicle which a driver cannot see in his/her rear-view mirrors. The system using sensors checking the blind spots and signal if any vehicle is in the blind areas.</td>
</tr>
<tr>
<td>Longitudinal control</td>
<td>Distance keeping</td>
<td>The system keeps a distance, pre-set by the driver, to a leading car. If the leading vehicle slows down, the system will slow down its host vehicle so the safety distance set can be kept.</td>
</tr>
<tr>
<td></td>
<td>Speed control</td>
<td>The system controls stops the car from going faster than a set speed. The speed limit is either set by a driver or automatically according to local speed limits.</td>
</tr>
<tr>
<td></td>
<td>Collision warning</td>
<td>The system constantly scans the road for vehicles and other obstacles. If an obstacle is found, the system warns the driver if there is potential risk for a collision.</td>
</tr>
<tr>
<td>Vision enhancement</td>
<td>Night vision</td>
<td>The system uses an infrared camera to view the road in front of the car and show the images to the driver in a display. Hence the driver is able to continue driving in conditions of reduced visibility, e.g. darkness or fog.</td>
</tr>
<tr>
<td>Driver monitoring</td>
<td>Driver vigilance monitoring:</td>
<td>The system classifies the vigilance of a driver by fusing information received from several sensors, such as vehicle lateral position, steering wheel position, driver’s eyelid movement. If the system detects low vigilance, the system will warn the driver.</td>
</tr>
</tbody>
</table>

6.4.4 Reduced mismatch through lowered environment demands

Another way of reducing accidents is to reduce the demands which the environment puts on the JDVRS. A direction for such reduction is to make the
demands of the environment expected and reasonable. Expectation is critical to avoid the occurrence of accidents. There are a number of measures which have been applied to make environments expected and reasonably demanding. Table 6.2 contains some examples:

Table 6.2: Examples of measures which lower environment demands

<table>
<thead>
<tr>
<th>Category</th>
<th>Measure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Speed limit</td>
<td>Lower vehicle speed provides drivers with more time to respond to situations. The selection of speed limit considers both the condition of the road (e.g. geometry) and activities around the road (e.g. school).</td>
</tr>
<tr>
<td>Roadway design</td>
<td>Roundabout</td>
<td>Non traffic light controlled intersections are normally more demanding and unexpected than traffic light controlled intersections. However, setup and maintenance of traffic light controlled intersection is expensive. By using roundabouts for intersections, speeds are reduced for a relatively low cost, and demand and unexpectedness is reduced.</td>
</tr>
<tr>
<td>2+1 road</td>
<td></td>
<td>2+1 road is a specific category of three-lane road which consists of two lanes in one direction and one lane in the other, with this setup alternating every few kilometres. Since overtaking is possible in the two lane section, this reduces the need for demanding or unexpected overtaking manoeuvres.</td>
</tr>
<tr>
<td>Traffic sign</td>
<td>Dynamic message sign</td>
<td>The system, an electronic traffic sign, provides real time traffic information to drivers about things like traffic congestions, accidents, incidents, roadwork zones, or temporarily reduced speed limits on a specific highway segments.</td>
</tr>
<tr>
<td>Counter</td>
<td></td>
<td>A traffic light is equipped with a counter. The counter shows the time left for the current state, e.g. how many more seconds of red or green light.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Road</td>
<td>A well maintained road can reduce the chance of unexpected events. Broken or invisible signs and markings increase driver demand and unexpectedness.</td>
</tr>
<tr>
<td></td>
<td>Vehicle</td>
<td>A well maintained vehicle reduces the chance of unexpected events.</td>
</tr>
<tr>
<td>Culture</td>
<td>Driving education</td>
<td>A good driving education system teaches drivers to behave as informative to other road users as much as possible, e.g. making their own actions predictable and transparent by for example always using the turn signal, and always use it in good time.</td>
</tr>
</tbody>
</table>
6.5 Proactive Road Safety Approach (paper IV)

As accident models are a set of beliefs about accident occurrence and prevention, they will (usually implicitly) contain a model of what Human-Machine Interaction (HMI) is, as well as a model of the relation between Human-Machine Systems (HMS) and contextual conditions. Looking at the systemic accident models, they regard the occurrence of accidents as due to complex interactions between the performance of driver, vehicle and road getting out of hand while trying to cope with the environmental conditions. The mismatch between an environmental condition and the joint performance of driver, vehicle and road implies an underlying HMI model which regards driver, vehicle and road as a joint system. The complex interaction between driver, vehicle and road in coping with an environment condition implies that the cognition of the driver and the cognition of the joint cognitive system is context related.

As was discussed in Chapter 5 on approaches to accident prevention, the systemic accident model provides a good foundation for an integrated proactive and passive accident approach. However, as also pointed out by for example the HERMES methodology, for such an approach to work, it is very important that the underlying theoretical and empirical platform is explicitly formulated and described.

This must be done for two reasons. First, it is important to make sure that the platform used is consistent with the accident model selected, otherwise results will be confusing at best and worthless at worst. Second, and even more important, the platform must be formulated and described because otherwise the researchers will not have sufficient tools to work with. Accident models are of a fairly abstract nature in themselves, and they leave a number of issues undetermined regarding for example mechanisms of human behaviours. This means that as stand alone units, they do not give sufficient guidance for the setting up of studies in applied research. Hence, an integrated accident analysis and prediction based on the systemic perspective must meet the following demands (Adapted from Cacciabue, 2004):

- Both incident/accident analysis and incident/accident prediction must rest on a common empirical and theoretical platform which is consistent with the chosen accident model, and formulated in such a way that:

- The results of accident and incident analyses can support the conduction of accident/incident prediction, and
• The results of accident/incident prediction can refine the results of accident/incident analysis.

Systemic accident models imply an underlying model of HMI as a JDVRS and the cognition of the joint cognitive system as context related. The HERMES methodology suggests that the empirical platform can be built by means of the ethnographic studies and cognitive task analysis.

6.6 Future Research

As discussion in Chapter 5, a balance between accident investigation and accident prediction can provide a better performance than emphasizing on any individual of them. The details of such an approach need to be further spelled out. Moreover, as it should rest on an accident model, both the model and the accompanying empirical and theoretical platform needs to be developed and described. Much work has already been done on these things in other areas, but for road safety, there is still a lot to do and lessons learned in other domains to incorporate. Another interesting track for future studies regards the concept of variety. As the Law of Requisite Variety tells us - only variety can destroy variety. In road safety, we need to know more about the what the variety of complex processes (i.e. driving) and controller (i.e. JDVRS) looks like, and how they can be matched to the environment.

6.7 Concluding Remarks

Heinrich’s safety management approach pointed out the importance of accident models. Normal accident theory pointed out that accidents in complex systems are caused by complex interactions between component failures rather than individual component failures. Cognitive Systems Engineering stresses that the study of human-machine systems should take a systemic view. From this theoretical background, this thesis has explored the field of road safety theoretically and analyzed road incidents/accidents empirically. The results of the theoretical study suggest that systemic accident models can provide a better understanding of the complexity and dynamics of modern road accident processes.

Moreover, such an understanding benefits the selection of countermeasures. The results of empirical studies support the results of the theoretical study. A network of factors has been identified from investigated cases (both accidents and near-
misses). Even in very straight-forward cases, the systemic concept “forces” the investigators and the analysts to dig deeper. There are some professional accident investigators and analysts who are not directly involved in the project but who have voluntarily participated in case analysis meetings held in the FICA project. They reflected that the analysis based on the systemic concept gave them a different view of accidents compared to what they were used to, and they are happy to have such a new pair of glasses.

It is my hope that these new glasses will spread in the road safety community, and that perhaps other researchers will make new glasses of their own. I have proposed a direction for the development of modern road safety, but there may well be other directions holding just as much promise. The important thing is not which accident model or prevention approach “wins”, the important thing is that the road safety community starts a discussion on whether the usual way still is the right way. To do this, basic concepts such as accident philosophies must be unearthed and brought forth for inspection and revision. Current road safety focuses on accident investigation and pays little attention on accident prediction. Since from a theoretical point of view, a balance between accident investigation and accident prediction can provide a better performance than emphasizing on any individual of them, it is probably time for a paradigm shift if we are to successfully prevent the road accidents of the future.
REFERENCES


