Human Error and the Failure of Imagination: A Preface to HESSD 2004

The papers in this collection address the problem of developing systems that support human interaction with complex, safety-critical applications. The last thirty years have seen a significant reduction in the accident rates across many different industries. Given these achievements, why do we need further research in this area?

There is little room for complacency. For example, it has been difficult to sustain reductions in the incident rate across the aviation industry. This not only indicates an impasse in attempts to achieve 'zero' accidents. It is also a source of long-term concern because a stable incident rate combined with rising numbers of departures will yield increases in the frequency of adverse events. In other areas, the incident rates are rising in spite of the best efforts of safety managers. For instance, the frequency and rate of serious accidents in the US Army declined steadily in the decade prior to 2000. However, since that time there has been a rise in the number of soldiers killed or seriously injured by these adverse events. The nature of military operations has changed over this interval. Not only have operations in the Middle East increased risk exposure but the changing technology used by personnel has also affected the nature of many adverse events. In May 2003, Defense Secretary Rumsfeld focused concern: "World-class organizations do not tolerate preventable accidents. Our accident rates have increased recently, and we need to turn this situation around". He set the challenge to "to reduce the number of mishaps and accident rates by at least 50% in the next two years".

The US Army has recently established a number of initiatives that are intended to reduce the frequency of adverse events. For example, the 'Safety Sends' initiative is using Internet communication techniques to update units on potential hazards. The latest update reported on the fatal accidents from 8 March 2004 to 8 April 2004, 29 'Class A' mishaps resulted in 25 fatalities. 26 were ground incidents. 19 of these related to vehicle accidents and these accounted for 18 fatalities. 11 soldiers were killed in Privately Operated Vehicles. 4 of these soldiers were not wearing seatbelts. One soldier fell asleep at the wheel. 3 HMMWVs, an LMTV, and an M2 Bradley were involved in rollover accidents with 6 fatalities. There were 3 physical training related fatalities over this 4-week period. An important observation is that these accidents form part of a wider pattern in which most US army personnel are killed in road traffic accidents and in which 'roll over' incidents remain a continuing cause of injury. There are few surprises in this data.

It is, therefore, paradoxical to argue that many accidents and incidents stem from a 'lack of imagination'. The personnel involved failed to predict that their actions could place them and their colleagues at risk. Designers place operators at risk through this same lack of imagination; they do not anticipate the many diverse ways in which complex systems will be operated within their working environment. As we shall see, many of the contributions in this volume describe what happens when either the operator or systems designer fail to imagine the possible hazards associated with safety-critical applications. Recent accident reports provide further evidence to support this argument. For instance, the Gunner of a Bradley fighting vehicle was found unconscious from the start of carbon monoxide poisoning. The investigation later found that the soldier had been riding half in and half out of the overhead troop hatch. This was the exact location where the highest concentration of carbon monoxide was found. It was also discovered that the soldier was a smoker and hence may already have had elevated levels of carbon monoxide in their bloodstream. Subsequent investigations also revealed that the driver of the vehicle had discovered the seal on the engine panel was crimped but failed to recognise it as a potential hazard. The crew chief had also noticed problems with the seal and that a visible black 'streak' had been left by the blow back from the engine. After the incident, a motor pool mechanic found that the coupling between the engine and exhaust could also have contributed to the incident. This incident illustrates the 'difficulty of imagination'. In the aftermath of the incident, it is too easy to argue with hindsight bias that the individuals concerned should have anticipated this course of events. Given the pressures of more complex working environments, however, it seems reasonable to ask whether we would really have predicted the potential confluence of events that led a smoker to position themselves in the greatest concentration of carbon dioxide that stemmed from a loose exhaust coupling and was dispersed by a crimp in the engine panel seal. It is also important to reiterate that it is correspondingly more difficult to anticipate potential accidents involving human interaction with complex, distributed, computer controlled systems. The risks of carbon monoxide poisoning from a Bradley are relatively well understood when compared, for example, with the risks associated from night vision devices or from interaction with Unmanned Airborne Vehicles.

The previous paragraphs have argued that many accidents occur because operators and designers do not imagine the manner in which a complex, safety-critical system can fail. It follows, therefore, that good design depends upon the ability to imagine and then respond to these potential failure modes before they occur. The word 'imagination' has strong links with terms such as 'subjectivity' and individual 'creativity' that are not normally associated with the engineering of safety-critical systems. In contrast, objectivity is often seen as a prerequisite for the certification, validation and verification of potential designs. It is for this reason that many of the papers in this collection present techniques that are both intended to help designers anticipate potential hazards and then document the reasons for their predictions. Imagination and domain expertise are essential to identify failure modes. For instance, Johansson et al describe how critiquing tools can be used to provide teams with the ability to identify potential problems before they occur. However, analytical methods must then be recruited to document the basis for any risk assessment. Karsten et al and Jambon et al go on to provide examples of the way in which formal methods can be used to represent and reason about risk mitigation techniques.

Critiquing tools support the designer's 'imagination' in ways that can be used to identify potential failure modes. Semi-formal and formal methods can be combined with risk assessment techniques to arguably provide the objective rationales that support certification and design. However, a further strand of papers in this collection point to the limitations that affect these analytical techniques. In particular, their use needs to be closely informed by operational experience. For example, a recent incident occurred when fuel contaminated the oil of another Bradley. This reduced the lubrication available to the engine and it seized. The driver tried to continue. A rod tore through the bottom of the oil pan, taking part of the engine block with it. Friction ignited fuel residues and an explosion blew part of the engine compartment panel into the driver. He was stunned but managed to exit through the driver's hatch. The rest of the crew heard the driver yell 'fire' and the troops in the back of the vehicle tried unsuccessfully to open their exit ramp. The driver heard them and returned to his cab to operate the ramp. Within 15 minutes the fire reached the live 25mm ammunition and TOW missiles. The Bradley was destroyed but nobody was injured. This incident is instructive because the battalion commander had performed a risk assessment using techniques that are similar to those advocated within this collection. In consequence, he had successfully identified vehicle fire as a hazard. When investigators reviewed the unit's risk mitigation guidance, there was no reference to crews rehearsing vehicle fire drills, as described in applicable manuals. The occupants of the destroyed Bradley didn't understand the vehicle's fire suppression system. The command had properly identified the hazard, but failed to properly assess it and provide proper control measures to reduce the risk. Hence, as Andersen and Gunnar argue, risk assessment is insufficient unless adequate barriers are deployed.

This incident is also instructive because it also acts as a reminder of the relationship between risk assessment, design and human error. At one level, the Bradley's crew failed to follow standard operating procedures because they did not deploy the vehicle's fire suppression systems. Similarly, there should have been closer coordination in evacuating the troops in the back of the vehicle. However, as Nasrine et al and Urs point out human error analysis is seldom so straightforward. After the Bradley incident the enquiry did not emphasise the crew 'errors'. There are good reasons why investigators emphasised the need to practice using the fire suppression systems. The Bradley has two different applications. The first protects the squad compartment. The second separate system is installed in the engine compartment. Each has separate fire bottles. The ones for the squad compartment are next to the turret, while the fire bottle for the engine compartment is underneath the instrument panel. As mentioned, these systems are independent. If one system is activated then it will not automatically start he other. The squad system can be set to work in either automatic or manual mode. In automatic mode, the system will discharge a Halon suppression agent from the two rear fire bottles as soon as the sensors detect a fire. The system can be activated manually by pulling the fire extinguisher handle in the right rear of the squad compartment or by pulling a handle outside the vehicle. The need to practice using these systems stems in part from the adverse effects that Halon discharge can have upon the occupants of the vehicle if they do not exit in sufficient time. In contrast, in order to operate the engine fire suppression system the driver must first shut down the vehicle and reach under the instrument panel. They must then turn a dedicated lever to the left or they can pull on a handle outside the driver's hatch.

Several of the papers in this collection, including Turnell et al, Johnson and Prinzo, make the point that risk assessments must be informed by a close analysis of the working practices and management structures in end-user organisations. The previous incident provides a further illustration of this point; the Battalion commander identified the hazard but failed to mitigate the potential consequences by ensuring adequate training. This incident also illustrates a number of further issues that are addressed in this collection. In particular, the papers by Nisula, by Knight et al by Isaac and by Bogner, all address the role of incident and accident reporting in the development of safety-critical interactive systems. The fire in the Bradley occurred because the lubricating qualities of the engine oil were compromised as a result of fuel contamination. A number of precursor events might have alerted personnel to the potential dangers. Another driver had been using the same Bradley and had performed a number of preventive maintenance checks. He identified a potential fuel leak and noticed fuel in the engine oil. Dismounted infantry had noticed a strong fuel smell in the crew compartment. Company maintenance personnel were informed but couldn't find the leak. They did find evidence of the oil contamination but the pressure of mission requirements forced them to return the vehicle into service. The crew attempted to deliver the vehicle to a field service point but this had been moved from its original location. The key point here is that the techniques and methods that are described in this collection can only be assessed within the context of the organisations that will use them. In this example, the army understood the importance of risk assessment as a means of structuring and documenting the necessary steps of 'imagination' that help to predict potential failures. Unfortunately, operational demands and the complex spectrum of risks that typify many military operations prevented adequate barriers from being developed. Similarly, the maintenance and operational personnel within the unit understood the importance of incident reporting. However, a complex combination of contingencies again prevented necessary actions from being taken to address the potential hazard.

To summarise, many accidents and incidents stem from problems that are well known to designers and to operators. However, many adverse events reveal a failure to 'imagine' the many different ways in which an incident could occur. This lack of imagination stems in part from attribution bias, we believe that others are more likely to be involved in adverse events than we are. It also stems from the complex ways in which component faults and operator 'error' combine to create the preconditions for failure. The papers in this collection provide techniques to address these problems, for example by extending the scope of human error analysis and risk assessment. We have argued, however, that these techniques will not be effective unless organisations scrutinise the resources that are devoted to mitigate risks once they have been identified. Other papers describe how incident and accident analysis can extend the scope of our imagination by providing important insights into previous failures. Again, however, organisational barriers often intervene so that these lessons can be difficult to act on in an effective manner.

The papers in this collection also offer a number of further insights. Firstly, they illustrate the generic nature of many of the issues involved in human 'error'. Different contributions describe overlapping aspects in aviation, robotics, maritime applications, the leisure industries, military operations, healthcare etc. Secondly, it might be argued that few lessons are effectively shared between these different domains. For example, the problems that were apparent in interaction with aviation navigation systems are now being observed in maritime applications. Thirdly, the papers in this collection help to identify useful national and international initiatives, for example Hart presents recent developments within the aviation industry to exchange data between countries. Similarly, Bogner presents similar work at a national level in healthcare. However, these pioneering industries are faced with considerable challenges. Rather than supporting a single national, or federal, system for reporting adverse events in healthcare, individual US states are developing separate schemes. These are often poorly integrated with existing Federal systems that are used, for example, to report device related problems. In consequence, clinical staff must choose between five or more different reporting systems when deciding to report an iatrogenic incident. Similarly, many European states perceive there to be a threat to national sovereignty when schemes are proposed to adopt common reporting practices across different air traffic management organisations.

The opening sections of this preface argued that unexpected combinations of well-known failures often surprise us. The middle sections of this preface described how the papers in this collection address this problem, by risk assessment, formal and semi-formal modelling and by incident analysis. The closing sections of the preface have illustrated some of the organisational barriers that complicate the use of these techniques. The final paragraphs have opened up this critique to identify some of the political and structural issues that can hinder work in this area. This conference cannot hope to address all of these issues. We have opened up a dialogue in previous meetings now it is time to establish a clearer research agenda, in particular to determine how well many of the proposed techniques would survive in organisations as complex as the US military.

Chris Johnson and Philippe Palanque, 18th May 2004.