UNDERSTANDING HUMAN ERROR IN CONTEXT: APPROACHES TO SUPPORT INTERACTION DESIGN USING AIR ACCIDENT REPORTS

Dr Anne Bruseberg and Prof Peter Johnson
Department of Computer Science, University of Bath
Bath, UK

Producing a deeper understanding of the ways in which human operators and technical systems have failed to collaborate in the past is one of the main sources of insight for designing safer systems. Accident reports are a vital source of information for interaction designers – by providing detail about how design oversights may relate to human errors. Using such information requires a complex reasoning process to understand the accident sequence and interpret the facts available. This paper explores ways in which to gain a deeper understanding of the underlying reasons for human error from accident reports, in order to identify interaction breakdowns between operators and interfaces. It demonstrates an approach for examining contextual information of human error and deriving design ideas through an informal analysis. Having re-examined the Cali Air accident report in depth (Aeronautica Civil, 1996; Kaiser, 1996; Simmon, 1998), a more comprehensive understanding of the design problem space could be gained by relating a detailed understanding of the accident to design options. Moreover, the information available was captured in an accessible format to inform interaction design more effectively.

Introduction

Failures of human operators to deal with the demands of controlling complex systems, such as automated aircraft, has become a major contributor to accidents. The number of accidents to which high workload situations were a significant contributory factor (e.g. Bangkok, Cali, Strasbourg) is a cause for concern. To be able to design safer systems, interaction designers need to understand the role that automated functions and human-computer interfaces may have played in contributing to unsuitable operator actions leading to incidents and accidents. Accident reports are an essential resource to understand interaction failures between systems and operators. Accident data provide insight into concrete problems, and offer real task scenarios to understand them in complex operational and environmental contexts. This supports requirements analysis, conception of design solutions, as well as evaluation.

Interaction designers rely on information from existing accident reports, which do not specifically aim at informing interaction design. Designers require insight that accident reports do not primarily focus on. Identifying 'design errors' beyond 'operator errors' requires a detailed examination of the complex context in which errors occurred. The analysis relies on tracing the beliefs and thinking processes of pilots when failing to deal with the situations that evolved during the course of the accident, in relation to contextual factors such as external conditions, aircraft actions, automation logic, or human characteristics.

Making accident data accessible for design

Utilizing accident reports to inform interaction design is a complex task. Accident sequences are a unique combination of circumstances. The analysis requires understanding a multifaceted process retrospectively. Moreover, accident reports aim to establish a wealth of facts and do not specifically aim at informing interaction design processes in depth. They aim to provide a concise list of basic recommendations for different audiences. Their format and focus makes them difficult to use directly by interaction designers.

For example, the line of reasoning might be distributed across several different pages in a lengthy document, thus making it difficult to reconstruct the conclusions from the evidence (Johnson, 1998). Johnson (1999) suggests the use of CAE (Conclusions, Analysis, and Evidence) diagrams, to be able to track the reasoning behind accident reports. Leveson (2001) advocates exploiting the opportunities given by the complexity of accident processes for identifying preventative measures, rather than attempting to find simplistic explanations. Likewise, ambiguity may occur through biasing expectations, or through choice of emphasis (Snowdon & Johnson, 1998).

Traditionally, causal analyses are often driven by trying to establish accountability in a legal sense. Leveson (2001) found that accident reports often focus on assigning blame rather than presenting the diversity of the evidence. Moreover, reports were found to try and oversimplify the conclusions to few major factors, rather than investigating the complexity of the factors – thus introducing a process of subjective filtering. These issues were found to

make standard reports less valuable for dealing with engineering issues.

The approach presented here shows how the material gained from accident reports can be made more accessible and usable for interaction design. It demonstrates how the reasoning process of the analysis may progress to inform the generation of design ideas.

Identifying interaction design options

Events in the accident sequence can often be attributed to a number of different causes. The likelihood of their re-occurrence can be decreased through a number of complementary design measures (e.g. design, training, crew procedure, air traffic control behavior). For example, during the Cali Accident (Aeronautica Civil, 1996; Kaiser, 1996; Simmon, 1998), one of the major errors made was the faulty input of the waypoint 'Romeo' into the FMS, instead of 'Rozo', thus taking the aircraft off course into mountainous terrain. A number of different design opportunities can be specified for this problem – to deal with it from different perspectives, all of them having potential value:

- *Organisational design (causing external pressure):* The time pressure due to the delay forced the pilots to hurry their actions, thus violating standard procedures;
- *Organisational design (naming of radio beacon)*: There should not have been two NDBs (waypoints) with identifier 'R' in the same area;
- *Training design (area information)*: the crew should have been made aware that 'R' does not call up Rozo in the FMS, but only input of 'ROZO';
- *Database design*: The charted and FMS databases should have presented identical information;
- *Interface design*: The list of NDBs displayed as options to select from was difficult to interpret at a glance, since given as Latitude/Longitude only;
- *Interaction design*: The communication process between FMS and pilot to enter instructions did not force the pilot sufficiently to re-consider his input;
- *Training design (decision making skills)*: The crew should have been given additional training in how to properly review actions before making hasty decisions about route changes.

Accident analyses often focus on establishing major causes that have more weight than other contributory factors. However, there is no guarantee that a 'minor' cause from one accident cannot become a 'major' cause in another. Thus, influencing any of the factors can make an improvement. It is essential to consider the complete picture, since there are always multiple 'root causes', leading to a range of potential design opportunities. Moreover, Leveson (2001) notes that the distinctions made between 'root' and contributory causes are often made on a subjective basis. Along these lines, Haddon (1967) argues that defenses should not be chosen according to the relative importance of causal factors, but the effectiveness of associated measures in preventing future losses. This paper focuses on how to identify potential contributions to safer systems through interaction design. The analysis process aims at identifying design *opportunities*, rather than a narrow list of design requirements.

The need to understand errors in context

It is often difficult to distinguish between system failure and operator error, and the way they interact (Johnson, 1998). Accident reports have a tendency to identify adverse events in relation to human failures. The way errors are formulated is often based on the observation that pilots have not followed procedures that had already been in place (e.g. checklists, communication procedures), or preferred paths of actions that were identified through hindsight. The focus on operator error can divert attention from oversights made in the past, such as maintenance, designer, or manager error. Moreover, re-considering interface design is often considered to be the more long-term and more costly option.

Wiegmann & Shappell (2001) present a framework for identifying and classifying the human causes of aviation accidents, based on Reason's 'Swiss cheese model' (Reason, 1990) – showing how operator errors can be traced back to the absence of suitable defenses, due to aspects such as substandard operating conditions or practices, unsafe supervision, and organizational influences. However, little is known about the latent errors that may have happened during the interaction designing process. A better understanding of the different types of 'design errors' is vital to guide designing processes.

The concept of identifying operator error lends itself much easier towards training and organizational recommendations, than understanding the underlying reasons of interaction failures. Similarly, Leveson (2001) expresses caution towards using the concept of human error. Since human error tends to be a deviation from an established norm, typical human performance is prone to constant error, since procedures cannot anticipate all required task variations. Moreover, accident analyses always identify errors through hindsight.

Understanding the nature of human error

Errors never happen in isolation. The underlying reasons for errors need to be traced by understanding the situations that lead to them, and by appreciating all the steps in the task sequence. A particular error leads to a new, unwanted situation and therefore to new requirements for counteracting unwanted effects. Failure to do so is usually identified as another error. Thus, understanding errors within the broad context in which they occurred is essential to find ways in which the interface can support the interaction.

It is important to not just focus on the unsuitable actions taken (or actions not taken), but more importantly, to comprehend the underlying misperceptions that lead to them. Evaluating an action as an error relies on an understanding of a 'better' path of action, usually retrospectively. Many erroneous actions (apart from slips and lapses) are based on faulty beliefs (e.g. goals to be achieved, current situation). Therefore, an understanding of the states of knowledge that led to the 'wrong' choice of action in a given situation is vital to understand the causes for human error. For example, the information that the pilots selected a flight path that lead to a collision with a mountain range does not help to understand the causes of the accident without having detailed knowledge of the erroneous understanding of the pilots regarding the position of the plane (e.g. the pilots believed that they had not passed the waypoint Tulua yet, and therefore were not as close to the mountains). Hence, the analysis needs to capture the incorrect comprehensions that pilots held prior to making errors, and after making errors. These follow causal chains just as errors do, and are closely related to them. However, analysts may only be able to speculate about them – hence it is difficult to establish proof for them.

Part of understanding errors in context is to understand the task during which errors occurred. Errors are embedded in cognitive activities, for which standard patterns can be identified (e.g. understand evolving situations, assess implications and action requirements, plan potential actions, execute actions). They have been described through a range of cognitive models – for example Rasmussen's decision ladder (Rasmussen, 1976). Moreover, a large proportion of pilot activities in glass cockpits focus on interacting with a computer-based agent (e.g. autopilot, flight management system). Thus, it is useful to consider the different types of pilots' interaction tasks during which errors can occur. They may be described through the following task elements – to be able to specify a range of potential interaction failures:

1 Developing an understanding of system status, including
   - Perceiving system alerts (e.g. failure to recognise alarm);
   - Observing/evaluating results of previous actions (e.g. failure to recognise system reactions);
   - Maintaining and updating awareness to identify undesired processes (e.g. failure to identify unexpected system parameters, the effect of external conditions, or mode changes);
   - Diagnosing – after something went wrong (e.g. failure to track fault; failure to recognise preceding errors).
2 Evaluating evolving system states to specify action requirements, including
   - Interpreting system information (e.g. failure to recognise the implications of events/actions/ conditions);
   - Prioritising goals (e.g. fixation on interaction with interface);
   - Considering system functioning and programmed goals (e.g. failing to understand automation procedures);
   - Mentally simulating future hypothetical situations (e.g. failing to take all restrictions into account);
   - Identifying need for interventions (e.g. failure to cancel descent after loss of location awareness);
   - Identifying procedure or action plan (e.g. unsuitable match of situation with procedure; omission of procedure).
3 Initiating system changes (e.g. wrong execution: slips, lapses; faulty execution of procedure; failure to communicate intentions and actions).

During a particular accident sequence, errors can occur during any of these activities. Since activities are interconnected, a whole series of errors may inevitably lead to each other. Rather than specifying individual errors, and simply labeling errors using error taxonomies, this suggests the need to identify multiple error paths, to be able to pinpoint unsuitable actions within their context.

All these types of activities determine specific design requirements. For example, an error to perceive an unexpected mode change by the system, or the failure to notice an alarm, raises questions of how to focus pilots' attention towards important events in an environment of information overload. However, interpretation, prediction or diagnosis activities

require a different type of support by the interface – for example by disclosing knowledge about the system functioning and providing advisory functions (Vicente & Rasmussen, 1992). Moreover, input dialogues need to support efficient communication of intentions and give pilots suitable opportunities to review the implications of interventions (Hourizi & Johnson, 2001).

Approaches to establish design opportunities from accident reports

Designing is a process of continual exploration. Creativity requires dealing with ill-defined problems (Cross, 2000). This means that achieving to fully understand the design task is part of the problem solving process. Hence, there is no distinct borderline between identifying requirements and specifying solutions, as one activity flows into another. Hence, a detailed exploration of design requirements and the problem space should be part of the interaction design process – or the reasoning behind the requirements specification should at least be traceable by designers. Moreover, the understanding gained through the accident analysis needs to support brainstorming for design options as an essential design activity. At the earliest stages of requirements specification, the analysis should support the identification of a range of design opportunities, rather than narrowing down the problem space to an essential list of recommendations – as is often the main objective of accident reports.

Accident analysis usually involves filtering of the available information to focus on the factors that contributed negatively to the course of events. A range of different factors needs to be understood including

- Pilot actions (e.g. reading map display, selecting new flight path angle, avoidance manoeuvre);
- Errors (e.g. selection of wrong heading, late decision of captain to go around);
- External events and conditions (e.g. low visibility due to darkness, no availability of radar from ATC, presence of high mountain ranges close to approach path, significant delay of plane);
- Restrictions guiding pilots' actions (e.g. regulations, procedures, standards);
- Beliefs that pilots held at the time (e.g. position of plane in relation to waypoints);
- Lack of knowledge and understanding (e.g. absence of full reverse thrust was not noticed);
- Resulting undesirable situations (e.g. distraction, 'soft' landing in heavy rain failing to reduce speed on touchdown);
- Statements about resulting problems (e.g. high workload, loss of situational awareness, rushed approach, airspeed to high, impact with mountain).

A wide variety of accident analysis techniques are available – both to establish facts and insights to produce accident reports, as well as to re-examine existing accident reports for more specific objectives. Livingston *et al.* (2001) provide a review of techniques available to identify 'root causes' for accidents. Accident analysis is a complex process that requires several levels of interpretation from the facts towards the conclusions. The analysis needs to be progressed through a number of stages, typically involving the following questions:

1. What happened?
2. What went wrong?
3. What were the reasons for the problems?
4. What are opportunities for future defences?

Many techniques fail to recognize the need for these different levels of interpretation processes, thus making the analysis process more complex.

When establishing what happened, the analysis should consider actions and events only – thus concentrating on the 'plain' facts, as provided by the accident report. It is essential to establish an understanding of the sequence of events over time (e.g. timeline). Understanding the implications of time is important to realize the sequence, proximity, and concurrency of events. Statements about factors such as conditions, situations, or mental states should be avoided at this stage, since they already imply an evaluation. However, it may be useful to summarize events (e.g. 'an agreement was reached'), thus starting off the interpretation process.

From this understanding of events, the analyst may then identify what went wrong. The process of interpreting the accident sequence requires analysts to abstract from facts towards conclusions. For example, a statement about high workload is a conclusion based on other insights. Likewise, identifying 'errors' means evaluating what operators have done in relation to what they should have done. Identifying unsuitable actions as 'errors' means considering alternative, preferable paths of events. Moreover, it is useful to establish smaller units of concern by grouping errors around those that had a major influence on the course of events. Table 1 shows an extract of the analysis for the Cali Air accident in an informal table format. Each row captures information for an error group related to a particularly influential error, thus reducing the

complexity of the analysis problem by being able to focus on a sub-problem only.

Next, problem causes need to be examined, thus investigating the 'errors' identified in context – by considering both their immediate causes and implications. Here, the focus should be on what happened, not on what should have happened. Columns 2 and 3 in Table 1 show a list of some of the implications and pre-conditions identified from the Cali accident report. These can include a wide variety of factors (e.g. conditions, situation assessments, pilots' beliefs).

This understanding of context can then be used to brainstorm about possible defenses, and thus design opportunities. Considering design oversights involves reflecting on how to influence any of the accident factors identified by taking alternative hypothetical outcomes into account. Design opportunities identified from the Cali accident are listed in the last column in Table 1. Figure 1 visualizes how error groups may be considered in their context of causal factors and implications, and how design oversights may relate to accident factors. It is essential to recognize that the analysis requires a multi-dimensional representation that is very difficult to achieve through two-dimensional graphical presentations, as used, for example, by Why-Because-Analysis (Gerdsmeier *et al*., 1997). The table format presented here supports the different interpretation stages and allows representation of a complex problem. If represented graphically, it would expand to a multi-dimensional picture.

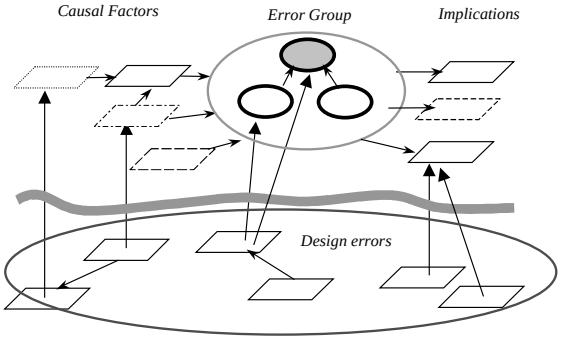

Figure 1: Linking an understanding of the accident to design opportunities and potential design solutions.

Conclusions

Understanding interaction design problems relies on an in-depth investigation of the different types of accident factors that lead to mis-communications between interface and pilot. Thus, human errors cannot be understood without a detailed examination of the context in which they occurred, since the concept of 'error' may otherwise create pre-conceptions towards potential solutions (e.g. training only). A detailed understanding of the task context is essential. Likewise, it is vital to examine the goals and beliefs that pilots held at the time of making errors, as they are critical to be able to understand the paths of unsuitable actions that unfolded. The approach presented here provides an informal way of investigating and presenting accident factors by placing them in their context, and considering the different levels of interpretation required to deal with complexity of the analysis task.

Acknowledgments

This work is being funded by the EPSRC (grant number GR/R40739/01) and supported by QinetiQ and Westland Helicopters.

References

Aeronautica Civil of the Republic of Colombia. (1996). AA965 Cali Accident Report, Near Buga, Colombia, Dec 20, 1995: available from: http://www.rvs.uni-bielefeld.de/publications/ Incidents/DOCS/ComAndRep/Cali/calirep.html.

Cross, N. (2000). *Engineering Design Methods: Strategies for Product Design* (2nd ed.). London: Wiley.

Gerdsmeier, T., Ladkin, P., & Loer, K. (1997). *Analysing the Cali Accident With a WB-Graph.* Human Error and Systems Development Workshop, Glasgow, March 1997, avail. from http://www.rvs. uni-bielefeld.de/publications/Reports/caliWB.html.

Haddon, W. (1967). The prevention of accidents. In D. W. Clark & B. MacMahon (Eds.), *Preventitive Medicine* (pp. 595). Boston: Little, Brown, and Company, cited in Leveson, 2001.

Hourizi, R., & Johnson, P. (2001). Beyond Mode Error: Supporting Strategic Knowledge Structures to Enhance Cockpit Safety. In A. Blandford & J. Vanderdonkt & P. Gray (Eds.), *People and Computers XV - Interaction without frontiers. Joint Proceedings of HCI2001 and ICM2001, Lille, 10-14th Sept. 2001* (pp. 229-246): Springer Verlag.

Johnson, C. W. (1998). Representing the Impact of Time on Human Error and Systems Failure. *Interacting with Computers, 11*(September), 53-86.

Johnson, C. W. (1999). *Using CAE Diagrams to Visualise the Arguments in Accident Reports*: Department of Computing Science, University of

Glasgow, Glasgow, G12 8QQ, available from: http://www.dcs.gla.ac.uk/~johnson/papers/cae_99/.

Kaiser, J. (1996). Flight 965, Accident Investigation Summary, APA Flightline - November 1996 - Special Report. avail. from http://www.alliedpilots.org/pub/flightline/nov-1996/flt-965.html.

Leveson, N. (2001). *Evaluating Accident Models Using Recent Aerospace Accidents*: NASA Internal Study, avail. from http://sunnyday.mit.edu/ accidents.

Livingston, A. D., Jackson, G., & Priestley, K. (2001). *Root causes analysis: Literature review*: HSE contract research report 325/2001, avail. from: http://www.hse.gov.uk/research/crr_pdf/ 2001/crr01325.pdf.

Rasmussen, J. (1976). Outlines of a hybrid model of the process plant operator. In T. Sheridian & G. Johannsen (Eds.), *Monitoring Behaviour and Supervisory Control* (pp. 371-384). New York: Plenum.

Reason, J. (1990). *Human error*. New York: Cambridge University Press.

Simmon, D. A. (1998). Boeing 757 CFIT Accident at Cali, Colombia, Becomes Focus of Lessons Learned. *Flight Safety Digest, May-June*, 1-31, available from http://www.svt.ntnu.no/psy/ Bjarne.Fjeldsenden/Aviation/CaliAccident.pdf.

Snowdon, P., & Johnson, C. W. (1998). *The Impact of Rhetoric on Accounts of Human 'Error' in Accident Reports*: Technical report, Department of Computing Science, University of Glasgow, avail. from http://www.dcs.gla.ac.uk/~johnson/papers/rhetoric/rhetoric.html.

Vicente, K. J., & Rasmussen, J. (1992). Ecological Interface Design: Theoretical Foundations. *IEEE Transactions of Systems, Man and Cybernetics, 22*(4).

Wiegmann, D. A., & Shappell, S. A. (2001). *A human error analysis of commercial aviation accidents using the Human Factors Analysis and Classification System (HFACS).* DOT/FAA/AM-01/03. avail. from http://www.hf.faa.gov/docs/cami/0103.pdf.

Table 1: Extract of the Cali accident analysis (statements about pilots' beliefs in italics).

Major Factor	**Errors**	**Implications**	**Pre-conditions**	**Design opportunities**
1. Decision to accept runway 19	• Wrongly prioritizing goal to deal with delay over flight safety • Failure to adequately review situation prior to decision • Failure to adequately re-plan new approach • Failure to recognize that plane was too fast, too high and too close to runway	• Need to re-program FMS with new approach parameters • Less time available until landing (quicker approach without turning) • Extreme workload reducing attention to flight progress	• Significant delay of plane (2:21 hours on take-off) • Need to ensure crew rest periods • Need to ensure passenger satisfaction • *Knowledge of clear weather, calm winds*	• Aid to support quick situation review to enable critical planning process; issues of o Speed of accessing critical information o Information distribution o Advice facilities • FMS approach editing – speed of input; change of single parameters rather than all • Interaction design enabling to deal with sudden high workload
7. Failure to understand position and proximity of mountains	• Failure to familiarize with terrain information; use of approach chart (not local area chart) as primary reference • Failure to detect aircraft's deviation from path early enough • Failure to regain situational awareness • Failure to interpret signal from ULQ; failure to locate Tulua • Decision to intercept extended centerline to Cali/Rozo without understanding relation to terrain	• *Lack of awareness of dangerous situation (failure to appreciate terrain information in relation to the flight path)* • *Wrong belief of crew that Tulua had not been passed yet and the mountains where not as close* • Inability to identify significant turn away from course towards Romeo • *Belief that there is something wrong with Tulua locator*	• Darkness – no visual terrain cues • No availability of ATC radar coverage • Frequent radio contacts • Very limited time available to perform required tasks • Crew was rushed, disorientated and confused • Neglect to realize descent into unknown area • *Belief that interaction with FMS (i.e. locating Tulua, selecting CLO (Cali) to re-gain direction) helps*	• Mountain information available on different displays, not clear on main one • Accurate magenta line on approach chart may result in overconfidence in automation • Change of course was not made obvious enough to busy crew • Display did not enable pilots to locate plane under stressed, confused conditions o FMS did not clarify the situation o Signal from ULQ could not be interpreted having made wrong assumptions about location • Automation gave false sense of security through facility to input waypoint (Cali) that changed direction towards desired location without validating terrain proximity