INTERNATIONAL DESIGN CONFERENCE - DESIGN 2004
Dubrovnik, May 18 - 21, 2004.

INTEGRATING OPERATIONAL COMPLEXITY IN DESIGN PROCESSES AND IMPROVING DESIGN RISK IDENTIFICATION

K. Lauche, J.S. Busby and S.A. Bennett

Keywords: design process, complexity, risk identification, systems of systems

1. Introduction

The aim of this paper is to analyse the impact of simplifying strategies on the design of complex systems. These strategies are useful and often necessary to make the design process tractable – yet designers must somehow discard these when trying to identify the risks that arise when a design is put into operation. For example it may be necessary to treat the external influences on a design as sequential to make progress with the design, whereas in practice they can arise simultaneously. The problem is not that such strategies are wrong as such - design generally has to be conducted in conditions of considerable uncertainty, vagueness and sometimes contradiction. The problem is instead that, when the designer analyses the risks associated with the design, (s)he has to undo his or her commitments to such simplifying strategies. The difficulty is that, when it becomes second nature to draw on simplifying strategies, it can be increasingly difficult to remember or even know in the first place that they have been used. In this paper we discuss the use of simplifying strategies by analysing the Überlingen mid-air collision as an example of a complex system failure. Based on a review of the literature on simplifying strategies, we outline our methodology and analyse aspects of complexity in the event and potential simplifying strategies that underlie a design process. Finally we will lay out a method for improving risk analysis.

2. Simplifying strategies in design

There is a considerable amount of research on how designers' reasoning departs from strict optimisation. Designers sometimes satisfice, set limited problem boundaries, partition the problem and ignore interactions, specify in advance quantities that are in fact uncertain or abstract away from context [Simon 1981; Ball *et al* 1994]. The organisational context of design also makes search processes distinctly sub-optimal. However, these limitations seem defensible, given the vague and changing information that is often available during design processes. They also serve important purposes, such as making the design more robust to other people's actions than optimised designs would be. Design problems are often 'wicked' [Rittel & Weber 1973] or 'ill-structured' [Simon 1981] problems, so require heuristics strategies of some sort to deal with. Optimising design can also result in a lack of robustness to changes in the interface with other designs [Busby 2001]. The problem with strategies that remove complexity, in order to make design tractable, is that they close designers' minds to complexities that will still arise when designs are put into operation. This phenomenon is not specific to design, as humans generally have problems in perceiving and dealing with complexity [Dörner 1996]. They tend to think of complex causal relations in terms of simple chains, assume trends are linear rather than exponential, and find it hard to deal with feedback loops. The question is how we can help designers foresee systemic failure and deal with the limitations to their foresight.

3. Aviation context and method

The context for the paper is the design of the 'system of systems' involved in managing air traffic, and in particular avoiding the risk of collision during flight. A case study on the mid-air collision over Überlingen in 2002 has been used to determine the kinds of complexity that arise when such systems are in operation in their target environment, and to determine how aspects of this complexity can be hidden from the normal processes of risk identification during the design process. The general system of air traffic control has several aspects that naturally introduce complexity:

- The elements of the system are moving in three dimensions at high speed.
- The system is a large-scale aggregation of technical and social entities in the cockpit and on the ground, so its behaviour reflects a wide range of physical and social phenomena.
- There is no single designer or design organisation.
- The system consists both of original designs and layers of subsequent modification.
- The component technologies are highly disparate, and date from a range of different eras.

But these aspects are shared by a wide variety of intrinsically hazardous systems, so the conclusions we develop should be applicable more generally.

The analysis of the Überlingen mid-air collision was based on cockpit transcripts and a secondary analysis of public documents and other research [Bennett 2004], but we had no access to primary data about the individual intentions of the designers. The approach followed an organisational accident analysis method in that it involved developing a causal network of the pattern of events, analysing system defences that failed, characterising the different kinds of complexity, and stipulating how the identified complexities may have been obscured in the design process.

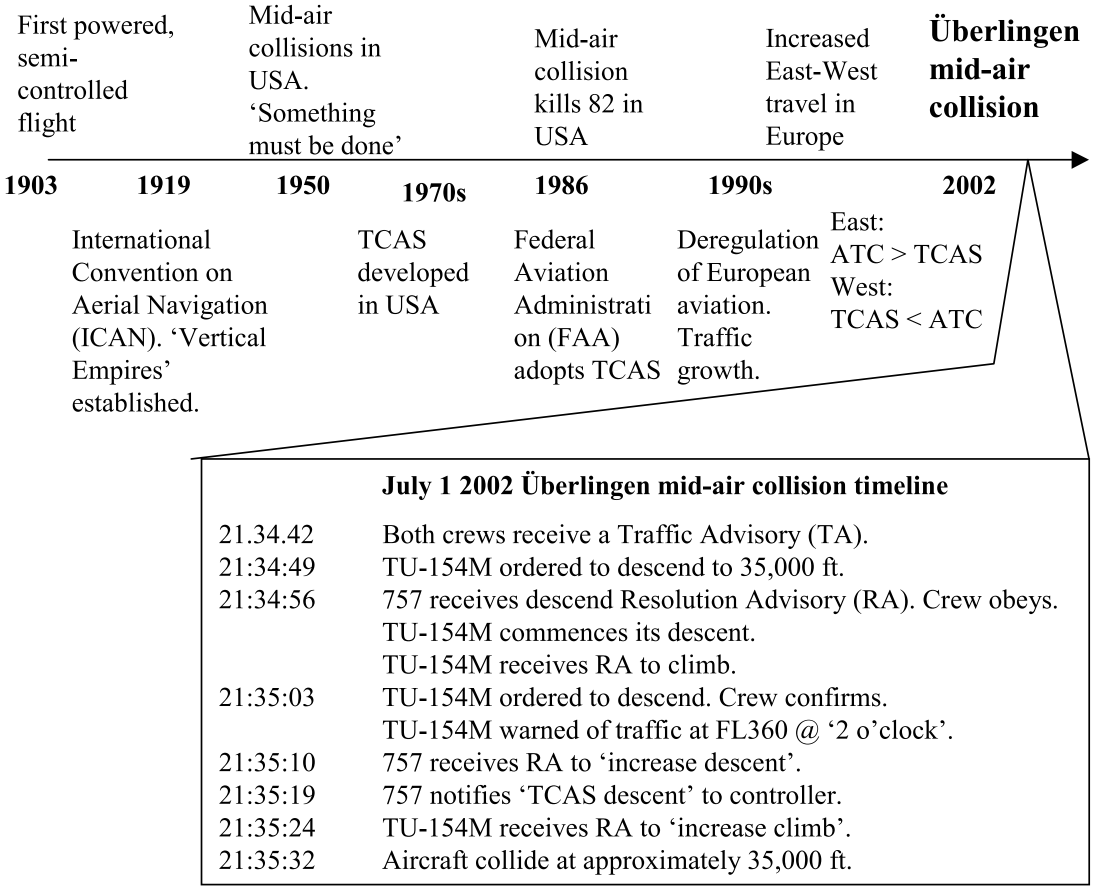
4. Reconstruction of the event

Figure 1 shows both the detailed events that preceded the collision, and the long-term history of the aviation industry that is relevant to it. On the night of 1 July, 2002 a Russian Federation-registered Tupolev 154M (Tu-154M) of Bashkirian Airlines carrying a party of schoolchildren collided with a Bahrain-registered DHL Boeing 757 cargo aircraft over the German town of Überlingen. Seventy-one persons died. At the time of the collision both aircraft were under the direction of Swiss air traffic control (ATC), which underwent scheduled maintenance and system update at the time to deal with increased air traffic. As a result, the radar system and the pre-programmed telephone connections were not fully available and the controller had to carry out several operations manually.

Both aircraft were equipped with an on-board anti-collision device known as Traffic Alert and Collision Avoidance System Version 2 (TCAS II). If TCAS II senses that two aircraft are on a collision course it issues reciprocal instructions to the crews. Its effectiveness depends on both crews obeying these instructions. While the DHL crew obeyed their TCAS instruction, the Bashkirian crew obeyed an air traffic control instruction that contradicted the advice issued by their TCAS unit. They consequently flew their aircraft into the path of the DHL aircraft. The collision shocked the commercial aviation industry and the various public bodies charged with its administration. It was the first European mid-air collision involving serious loss of life for some three decades.

As figure 1 indicates there is a historical and political background to the design of collision avoidance and its use. The consensus amongst several European Civil Aviation Authorities and the respective UN organisation was and is that TCAS instructions should take precedence over those issued by ATC. However, the advice offered by *international* bodies has no legal authority over sovereign nations. Also, the Russian Federation did not belong to any of the European regulatory agencies. Thirdly there is occasional ambiguity in the recommendations issued by such bodies, e.g. a crew might elect not to follow the instruction from TCAS [JAA 1998]. The procedure JAR-OPS 1.398 only specified that the pilot has to initiate corrective action to establish safe separation but it does not say the pilot has to follow the RA. The Mitre Corporation [Mitre 2003], one of the companies responsible for developing

TCAS, states that TCAS 'provides a backup to the air traffic control system's regular separation processes'.


First powered, semi-controlled flight
Mid-air collisions in USA. 'Something must be done'
Mid-air collision kills 82 in USA
Increased East-West travel in Europe
Überlingen mid-air collision
1903
1919
1950
1970s
1986
1990s
2002
International Convention on Aerial Navigation (ICAN). 'Vertical Empires' established.
TCAS developed in USA
Federal Aviation Administrati on (FAA) adopts TCAS
Deregulation of European aviation. Traffic growth.
East:
ATC > TCAS
West:
TCAS < ATC

July 1 2002 Überlingen mid-air collision timeline

21.34.42	Both crews receive a Traffic Advisory (TA).
21:34:49	TU-154M ordered to descend to 35,000 ft.
21:34:56	757 receives descend Resolution Advisory (RA). Crew obeys.
	TU-154M commences its descent.
	TU-154M receives RA to climb.
21:35:03	TU-154M ordered to descend. Crew confirms.
	TU-154M warned of traffic at FL360 @ '2 o'clock'.
21:35:10	757 receives RA to 'increase descent'.
21:35:19	757 notifies 'TCAS descent' to controller.
21:35:24	TU-154M receives RA to 'increase climb'.
21:35:32	Aircraft collide at approximately 35,000 ft.

Figure 1. The history of mid-air collision and Überlingen details

TCAS was designed to create confidence and certainty in situations of uncertainty and threat. For the technical design to function properly, it required that all nations integrate and operationalise TCAS in the same way. The necessary uniformity of interpretation and application was never achieved. The guidance on how TCAS should be implemented was ambiguous. Instead of dispelling uncertainty TCAS added to it. The fact that regulatory agencies' memberships were partial and that their advice could be ignored by sovereign states compounded the ambiguity and uncertainty surrounding the device. At the time of the Überlingen mid-air collision, the convention in Western Europe was the TCAS should be given priority over ATC. In Eastern Europe operating assumptions were *reversed*. The Russian Federation never saw TCAS as anything other than a decision-support tool in situations where there was no active air traffic control. The potential problem was known and discussed at the level of international organisations but it not consensus had been achieved at the time of the disaster.

5. Analysis

The analysis reviews the facts of the Überlingen disaster from a design perspective. As any accident analysis, this offers a unique opportunity to identify factors in a complex system that contributed to the accident trajectory with the benefit of hindsight. Not all of these factors may be known and identifiable in advance for those who design and operate the system, and there may be aspects of complexity that a single event cannot reveal. However, any event points to weaknesses in the system. The analysis does not claim to represent the original thoughts of the TCAS designers in the 1970s, or of those who designed international agreements about air traffic control, or planned the system update in Zurich. It remains a crucial challenge of any design of large complex socio-technical systems such as transportation that there are layers of history not easy to manage. This analysis is a stipulation of what may have contributed to the development of the disaster and how useful design strategies can add to the risk if they are not reviewed and challenged.

5.1 Aspects of complexity

TCAS and ATC provide two independent defences, which both act to separate aircraft in space. They can operate inconsistently and separate aircraft in different ways, but this only becomes problematic when the crews of the different aircraft make different assumptions about which sub-system should be given precedence. In this analysis alone one can see several kinds of complexity:

The existence of multiple defences in the system. Multiple, redundant defences are usually designed to achieve a higher degree of protection. Yet this multiplicity implies that those designing, operating and maintaining the system have more things to think about when planning their own defences. TCAS cannot be designed as though there were no ATC, for instance.

The existence of multiple organisations. The case involves interacting technical systems such as ATC, aircraft manufacturers and TCAS, as well as operating organisations such as airlines and international aviation agencies. The deregulation and increased traffic have made the relationship between these organisations even more complex. For the designers of TCAS this multiplicity and heterogeneity of organisations means a multiplicity of customs and conventions, of equipment types, diversity in training and experience among the people involved in the system etc.

The existence of multiple histories, cultures and associations. A pivotal condition at Überlingen was that the crews in the different aircraft made different assumptions about the precedence given to ATC and TCAS, based on different standards in East and West. The Western consensus was that TCAS should take precedence over ATC, but it was not a universal procedure. The fact that one of TCAS's developers describes TCAS is a backup to ATC's regular separation processes implies a different precedence relationship. One could argue that since there is a lot of consensus, problems like those encountered at Überlingen will be rare. However when the problem does occur the consequence can be catastrophic, so the design of the system as a whole should aim at extremely low probabilities rather than merely low probabilities.

The interaction of sub-systems in a contingent way. TCAS in combination with ATC only fails when there is diversity in the assumption about which should be given precedence. When this condition does arise, however, the defences are not merely ineffectual but positively hazardous. In the absence of TCAS this particular collision would not have arisen.

The degradation of parts of the system that removed defences progressively. Because of the system upgrade in Zurich, the telephone line to other centres failed, and although Karlsruhe observed the onset of the collision they could not communicate to ATC in Zurich. There normally is considerable redundancy in the system, but it is only effective if the system remains interconnected. Redundancy is almost a ubiquitous principle of protection in design – providing extra capacity beyond that necessary for normal operation, in case of extreme demand or a failure in the normal capacity. But certain patterns of degradation can evidently defeat this strategy.

5.2 Obscuring possibilities and simplifying strategies

The Überlingen case highlight the dangerous side effects that strategies and assumptions regularly used to make complex design problems tractable can have. The following list is a stipulation of simplifying strategies that the various system designers may have encountered.

- The **homogeneity strategy:** Designers often make the assumption that the conditions the system can explore are homogeneous with respect to a particular function being achieved. This means that specific conditions do not need to be enumerated and assumes that the design works in all of them. It seems to us to be a natural strategy to start a design process with. One needs to get to a specific design before one can examine how it will behave in different conditions, so it makes sense to start by conceiving of a design that only need work in the most frequent or most likely condition that will arise.

- The **redundancy-as-protection strategy:** Designers regularly use redundancy as the protective strategy and simply not examining whether it can be anything else. Redundancy of one sort or another is almost inevitably the basis for protecting a system, but – as in cases like this – may in fact introduce new failure paths.
- The **non-interacting-defences strategy:** Designers may assume that multiple defences are independent. This is related to the previous strategy, and allows one to protect a system to very high levels by adding more layers of protection rather than re-thinking the basic design of a system. It is a quick way of getting to very small failure probabilities because it allows the designer to multiply the failure probabilities of the various layers. It also allows the design of the defences to be subcontracted to different parties.
- The **pristine-system strategy:** Designers often starting thinking about how the system fails from its pristine state, rather than the state it might be in after some years of operation. Degraded systems can be worn, they might have been modified, and they can have non-functioning components and so on. But it is probably more straightforward when think about failure modes to take each component and not explicitly think of other parts of the system as being degraded at the same time.
- The **circumscribed-boundaries strategy:** In order to proceed with the design, designer often set the system boundaries in a way that makes inputs to the design process as certain as possible. This typically means setting the boundaries to exclude considerations such as how the social culture in the operating environment could undermine the designer's intentions Trying to reason about cultural influences is never likely to be very certain, in the way that reasoning about a physical system might be, and people designing technical systems often do not have the expertise to reason about social systems.

6. Implications for improving risk identification

Was Überlingen preventable and if so, was there anything a designer could have done? In the media and public opinion the blame for the disaster is often attributed to a single individual (the pilots, the air traffic controller on duty). The fact that many contributed to a complex system seems more difficult to accept. The problem of mid-air collisions was known and to many in the industry Überlingen came as a shock but not as a surprise. We believe that designers can and should contribute to the prevention of disasters like Überlingen by improving their method of risk identification. Research on complex problem solving generally showed that humans are not very good at anticipating the behaviour of complex systems yet can be prompted and trained to challenge and improve their own behaviour [Dörner 1996]. A method for improving the risk identification process would help designers articulate and question their simplifying strategies. It provides a way of supporting reflective practice [Schön 1983, Lauche 2001] in the specific context of risk analysis.

The method contains three main elements: an intentionality analysis, an examination of simplifying strategies, and a risk search. The **intentionality analysis** requires the designer to draw out a hierarchy or network of the goals associated with the design. Most qualitative risk analysis methods (such as HAZOP) require a statement of what the design is meant to do so that one can reason about departures from this intention. The value of expressing this intention in a hierarchy of goals is that risks can be identified and expressed at any level. In some cases, risks are most easily identified at a general level, but in other cases at a more specific level.

The **examination of simplifying strategies** requires designers, probably working collectively with peers, to examine the strategies they have applied to make progress with the design in question. This is easier said than done, so our proposal is that this is done with prompts, or guidewords, derived from analyses like our own. The previous section, for instance, presented some general categories of simplifying strategy that might have been used in connection with Überlingen, but plainly they are general enough to be found in any context.

The third element, **the risk search**, requires the designer to search for risks that involve deviations from the intended goals and objects of the simplifying strategies. For instance, part of the goal network for a collision avoidance system might be decomposed into the sub-goals of a) proximity detection and

b) action invocation (telling the pilot to climb or descend). At the same time, the second stage of the process (identifying simplifying strategies) might have revealed that one simplifying strategy that was being used in the design was to make arbitrary assumptions about where the boundary lay between the responsibilities of the collision avoidance system and the traffic control system. The object of this strategy is the system boundary: the strategy is, essentially, to treat this boundary in a simplified way. We therefore need to look for risks that implicate the system boundary in failing to achieve the goals we have enumerated. For example, in terms of proximity detection, do both TCAS and ATC perform this function, and if so is it obvious that one is more reliable than the other? In terms of invoking action, do both TCAS and ATC perform this function, and if so which should be given precedence? This might have helped reveal the failure mode that actually occurred.

There is no guarantee that a process like this will definitely reveal risks that arise from operational complexity. All risk analyses involve search processes that cannot be guaranteed. But a process like ours does serve to make it more likely that a given risk will be identified before it materialises.

7. Conclusions

Analysing disastrous events such as the mid-air collision of Überlingen highlight the problem of designing for complex systems with a history of technical and social idiosyncrasies. While it is natural and often functional to make simplifying assumptions during the design process, there is also a danger that the risks not anticipated might create an adverse impact. Therefore Überlingen makes a strong case for a risk identification methodology that involves the examination of simplifying assumptions. Risk identification as it currently stands simply asks the question ‘what risks can we envisage?’ It fails to ask the question ‘what are the underlying assumptions of our reasoning about risk? What is it we take for granted?’ These second questions are essential if designers find they have to make arbitrary, over-generalised or simplifying assumptions in order to make progress, and then have to reason about the risks of putting a design into operation. This work also provides a potentially important way of exploiting our descriptive knowledge of how designers design. It does not suggest that the strategies they sometimes use, like satisficing, should be abandoned – but instead that knowledge of such strategies should be considered explicitly in risk identification activity. Knowing how you simplify the world should make you better able to anticipate what kind of world will cause your designs to fail.

References

Bennett, S. A. "The 1 July, 2002 mid-air collision over Überlingen, Germany. A holistic analysis". Risk Management: An International Journal.2004, in print

Ball L.J., Evans J.St.B.T. and Dennis, I.." Cognitive processes in engineering design: a longtitudinal study". Ergonomics, 1994, 37, pp. 1753-1786.

Busby J.S. "Error and distributed cognition in design", Design Studies, 22, 3,2001, pp. 233-254.

Dörner, D., "The Logic of Failure. Recognizing and avoiding errors in complex situations", Basic Books New York, 1996

Lauche, K. "Heedful action, reflection and transfer in the design process", Proceedings ICED 2001, Glasgow, 2001, pp267-274.

Schön, D. A." The Reflective Practioner. How Professionals Think in Action", Basic Books New York, 1983.

JAA, "Temporary Guidance Leaflet No. 11 Guidance for Operators on Training Programmes for the Use of Airborne Collision Avoidance Systems (ACAS)", Central JAA Hoofddorp, Netherlands, 1998.

Mitre Corporation," Traffic Alert and Collision Avoidance System". http://www.mitre.org/, 27 May2003.

Rittel, HWJ. & Weber, MM. "Dilemmas in a general theory of planning" Policy Sciences, 4, 1973, pp. 155-69.

Simon, H.A., "Sciences of the Artificial", MIT Press Cambridge MA, 1981.

Dr Kristina Lauche
Industrial Psychology Research Centre, School of Psychology, Univerity of Aberdeen
Aberdeen AB24 2UB, Scotland UK
Telephone: +44 (0)1224 272280, Telefax +44 (0) 1224 273426, E-mail: k.lauche@abdn.ac.uk