An Extension of the Human Factors Analysis and Classification System (HFACS) for use in Open Systems

Harris, D. & Li, W-C.

Original citation & hyperlink:
Harris, D & Li, W-C 2010, 'An Extension of the Human Factors Analysis and Classification System (HFACS) for use in Open Systems' Theoretical Issues in Ergonomics Science, vol 12, no. 2, pp. 108-128.
https://dx.doi.org/10.1080/14639220903536559

DOI 10.1080/14639220903536559
ISSN 1463-922X
ESSN 1464-536X

Publisher: Taylor and Francis

An Extension of the Human Factors Analysis and Classification System (HFACS- X) for use in Open Systems

Don Harris and Wen-Chin Li

Department of Systems Engineering and Human Factors
School of Engineering
Cranfield University
Cranfield
Bedford MK43 0AL
United Kingdom

Psychology Department
National Defense University
No. 70, Section 2, Central North Road
Peitou
Taipei 112
Taiwan, R.O.C.

Abstract

The Human Factors Analysis and Classification System (HFACS), based upon Reason's model of human error in an organizational context is currently the most widely used human factors accident analysis framework, however it has been criticised for merely categorising accident data rather than analysing it. Previous research has established statistical associations between the levels and categories within HFACS but has not specified a mechanism by which one category influences subsequent behaviour. This paper extends the approach in two ways. Using the categories of control flaws derived from Leveson's Systems-Theoretical Accident Model and Processes (STAMP) approach it describes the mechanisms by which categories within HFACS are associated with other categories lower in the organizational hierarchy. It also provides a mechanism by which active failures can promulgate across organizations. The revised methodology HFACS-X (eXtended) is illustrated using the case study of the Uberlingen mid-air collision on 1 July 2002.

Introduction

Human error is now the principal threat to flight safety. In a worldwide survey of causal factors in commercial aviation accidents, in 88% of cases the crew was identified as a causal factor; in 76% of instances the crew were implicated as the *primary* causal factor (CAA, 1998). When investigating the human factors related causes the focus has now shifted away from investigating skill deficiencies and has moved toward other factors such as decision-making, attitudes, supervisory factors and organizational culture (Diehl, 1989; Jensen, 1997; Shappell, Detwiler, Holcomb, Hackworth, Boquet and Wiegmann, 2007). This change in emphasis has resulted in human error frameworks and investigation schemes being developed that analyse and categorise the organizational factors and psychological precursors surrounding the accident in an attempt to develop a more complete understanding of the circumstances and hence aid in the development of effective prevention strategies.

Background to the Human Factors Analysis and Classification System (HFACS)

The Human Factors Analysis and Classification System (HFACS) is currently the most widely used human factors accident analysis framework. HFACS is a generic human error-coding framework, originally developed for US naval aviation as a tool for the analysis of the human factors aspects of accidents. HFACS's development is described in a series of papers and books (e.g. Wiegmann and Shappell, 1997, 2001a, 2001b, 2001c, 2003; Shappell and Wiegmann 2001, 2003, 2004). It is based on Reason's (1990) model of human error. In this model active failures (which are the errors proximal to the accident, associated with the performance of front-line operators in complex systems) and latent failures (distal errors and system misspecifications, which lie dormant within the system for a long time) serve to combine together with other factors to breach a system's defences. As Reason (1997) observed, complex systems are designed, operated, maintained and managed by human beings, so it is not surprising that human decisions and actions at an organizational level are implicated in all accidents. Active failures of operators have a direct impact on the safety of the systems. However, latent failures are spawned in the upper levels of the organization and are related to its management and regulatory structures.

While Reason's model was extremely influential in the way that human errors were viewed in aviation accidents his model did not suggest remedial solutions. Based upon Reason's model, Wiegmann and Shappell (2003) developed the HFACS to service such a need. Although the system was originally designed as a framework for investigating and analyzing human error accidents in US military aviation operations (Wiegmann and Shappell, 1997), its authors have also demonstrated its applicability to the analysis of accidents in US commercial aviation (Wiegmann and Shappell, 2001a, 2001b; Shappell, Detweiler, Holcomb, Hackworth, Boquet and Weigmann, 2007), US general aviation (Shappell and Wiegmann 2003, 2004) and Australian general aviation (Lenné, Ashby and Fitzharris, 2008). Wiegmann and Shappell (2001b) claim that the HFACS framework bridges the gap between theory and practice by providing safety professionals with a theoretically based tool for identifying and classifying human errors in aviation mishaps.

The system focuses on both latent and active failures and their inter-relationships, and by doing so it facilitates the identification of the underlying causes of human error. However, aviation accidents are often the result of a number of causes and contributory factors, many of which have a human dimension to them (Baker, 1995) hence, the challenge for accident investigators is how best to identify and mitigate the causal sequence of events leading up to an accident. It is important to examine systematically the HFACS framework and identify if this framework is suitable to meet needs for aviation accident classification and investigation.

In recent years the HFACS system has been extended and adapted to analyse the underlying human factors causes in accidents involving remotely-piloted aircraft (Tvaranyas, Thompson and Constable, 2006) and as a basis for the analysis of General Aviation accident data by insurance companies (Lemeé, 2006). The method has also been developed to investigate maintenance error (HFACS-ME - Krulak, 2004) and a further adaptation of the system has been developed for the investigation of railroad accidents (HFAC-RR; Reinach and Viale, 2006). HFACS has also been used in the process for the prospective assessment of the effectiveness of aviation safety products developed as part of the NASA Aviation Safety Program (e.g. Andres, Luxhøj and Coit, 2005; Lechner and Luxhøj, 2005; Luxhøj and Hadjimichael, 2006).

The HFACS Framework

HFACS examines human error at four levels. Each higher level is assumed to affect the next downward level in HFACS framework. The HFACS framework is described diagrammatically in figure 1.

- Level-1 'Unsafe acts of operators' (active failures proximal to the accident): This level is where the majority of causes in the investigation of accidents is focused. Such causes can be classified into the two basic categories of errors and violation.
- Level-2 'Preconditions for unsafe acts' (latent/active failures): This level addresses the latent failures within the causal sequence of events as well as more obvious active failures. It also describes the context of substandard conditions of operators and the substandard practices they adopt.
- Level-3 'Unsafe supervision' (latent failures): This level traces the causal chain of events producing unsafe acts up to the front-line supervisors.
- Level-4 'Organizational influences' (latent failures and system misspecifications, distal to the accident): This level encompasses the most elusive of latent failures, fallible decisions of upper levels of management which directly affect supervisory practices and which indirectly affect the actions of front-line operators.

At the first level of 'unsafe acts of operators' errors represent the mental/physical activities of an individual that fail to achieve the intended outcomes. Violations refer to the wilful disregard for the rules and regulations that provide safety of flight (Reason, 1990). However, errors and violations do not provide the level of granularity required of most accident investigations. Wiegmann and Shappell (2003) expanded errors further into the four sub-categories of 'skilled-based errors', 'decision errors', 'perceptual errors', and 'routine and exceptional violations' (Figure 1). Routine violations tend to be habitual by nature and are often tolerated by the governing authority. On the other hand, exceptional violations appear as isolated departures from authority, and are not necessarily indicative of an individual's typical behaviour pattern, nor condoned by management (Reason, 1990).

Simply focusing on the 'unsafe acts of operator', linked to the majority of accidents, is like focusing on a fever without understanding the underlying illness that is causing it. Wiegmann and Shappell (2003) classified 'preconditions for unsafe acts' into seven sub-categories of 'adverse mental states'; 'adverse physiological states'; 'physical/mental limitations'; 'crew resource management'; 'personal readiness'; 'physical environment', and 'technological environment'. These can be regarded as what Reason (1990) described as the psychological precursors to unsafe acts.

The role of supervisors is to provide their personnel with the facilities and capability to succeed and to ensure the job is done safely and efficiently. Level-3 in HFACS is primarily concerned with the supervisory influence both on the condition of pilots and the operational environment. HFACS contains four categories of 'unsafe supervision';

‘inadequate supervision’; ‘planned inappropriate operation’; ‘failure to correct a known problem’, and ‘supervisory violation’ (Figure 1).

INSERT FIGURE 1 ABOUT HERE

The corporate decisions about resource management are based on two conflicting objectives, the goal of safety and the goal of on-time and cost-effective operations. It needs to be noted, though, that the decisions of upper-level management can affect supervisory practices, as well as the conditions and actions of operators. However, these organizational errors often go unnoticed due to the lack of framework to investigate them. These elusive latent failures were identified by Wiegmann and Shappell (2003) as failures in ‘resource management’; ‘organizational climate’ and ‘organizational process’.

Criticisms of the HFACS approach

Beaubien and Baker (2002) noted that it was often difficult to collect information about the latent conditions from incident or accident reports. Dekker (2001) suggested that the HFACS framework has only a slight link between human error and working environment and there is some confusion between categorization and analysis. He added that the framework merely repositioned human errors by shifting them from the forefront to higher up in the organization instead of finding solutions for them. Although HFACS was based directly on the organizational theory of failure promoted by Reason (1990; 1997) at the time it was derived there was little or no quantitative data to support the theoretical model upon which it was based. Recent work has, however, established relatively strong statistical relationships describing empirically the relationships between various components at the four different organizational levels in the analysis and classification system, giving support to the underpinning theory behind the framework. Data were obtained from the operation of uninhabited air vehicles (Tvaranyas, Thompson and Constable, 2006); military aviation (Li and Harris 2006a; Li and Harris, 2006b) and civil commercial aviation (Li, Harris and Yu, 2008). These studies have provided an understanding, based upon empirical evidence, of how actions and decisions at higher managerial levels within organizations may promulgate throughout them to result in operational errors and accidents. These associations between levels and components in the HFACS model, though, should not be interpreted as 'paths of causality', as in an event chain model of accident causation. They are better interpreted as 'paths of influence'.

Beaubien and Baker (2002) also originally criticised the validation evidence presented for supporting the utility of HFACS as it has all been collected and analysed by the authors of the system themselves. However, further data have now been published by other, independent users of the system (e.g. Li and Harris, 2005; Gaur, 2005; Tvaranyas, Thompson and Constable, 2006; Li, Harris and Yu, 2008; Lenné, Ashby and Fitzharris, 2008) supporting the assertions of the originators of the framework.

Nevertheless, HFACS does appear to overly focus on the last error made (as do many analytical techniques) and it doesn't easily accommodate the analysis of multiple errors. Aviation is an ultra-high reliability system that has developed in such a way that it is extremely unlikely that an accident can result simply from a single error. Resilient systems are characterised by the need for several breaches of system defences to occur before an accident may result. This should require many errors/failure before an accident occurs – not just a point of failure. Lemeé (2006) has criticised HFACS as when multiple errors are coded into the framework it does not accommodate the time and order of the sequence of events leading up to an accident. Such analyses can easily be performed when good data exist, usually for the events proximal to the accident (e.g. Multilinear Events Sequencing – Benner, 1975; or Sequentially Timed and Events Plotting – Hendrick and Benner, 1987) however it is a slightly unfair criticism of HFACS which takes a more systemic view of accident causation. Such event-chain based analyses can supplement an individual accident analysis but cannot be used to aggregate data over a number of analyses to identify wider-ranging, systemic issues. A generic, less fine-grained approach is also more suitable used where there is a paucity of data available (e.g. in the analysis of General Aviation accidents where these aircraft do not carry sophisticated flight data recorders or cockpit voice recorders).

Furthermore, not only are aircraft accidents rarely the product of a single error (many are the result of systemic failures) it is also not uncommon for errors made (when a chain of errors can be established) to reside in different organizations. HFACS cannot easily accommodate the effects of errors that promulgate across organizational boundaries.

Wiegmann and Shappell (2003) suggest that all extra-organizational factors take effect at level-4 (Organizational Influences) in the framework, and promulgate through the system from this point downwards. However, in the following section describing and analysing the Uberlingen mid-air collision, it will be demonstrated that this is not the case.

Commercial Aviation as an Open System

All industries are open systems (i.e. they must interact with their environment) and the aviation industry is no exception. As Schein (1992) stated: 'The environment places demands and constraints on the organization in many ways. The total functioning of an organization cannot be understood, therefore, without explicit consideration of these environmental demands and constraints' (p. 101). Open Systems Theory is derived from General Systems Theory (von Berthalanfry, 1956) although Katz and Kahn (1978) assert that this is not a theory but a framework within which the workings of a system may be better understood. They also argue that organizations are only selectively open, in that they interact with their environment but also need boundaries in order to exist. Katz and Kahn list the common characteristics of Open Systems, amongst which are that they import energy and resources from the environment; they have throughput (to transform these resources) and they output some of these transformed resources. Furthermore, Open Systems tend to be complex: they exhibit equifinality (many paths to same end) however to maintain a degree of control there is integration and coordination.

Central to systems theory are the two concepts of ‘emergence and hierarchy’ and ‘communication and control’ (Checkland, 1981). All complex systems are characterized by possessing a hierarchy of increasingly complex levels of organization with each higher level in the system possessing emergent properties not evident at the lower levels. Higher levels in a system constrain the degree of freedom to act on the components lower in the system hierarchy (qv. the organizational levels expressed in HFACS; higher managerial levels constrain the actions of the supervisory levels, which in turn constrain the actions of the pilots flying the line). With regard to the second concept, ‘control’ in systems theory is always associated with the imposition of constraints to act. In Open Systems such as an airline, control requires communication within and without the organization (Checkland, 1981). Notions of ‘communication’ and ‘control’ within the organization are implicit in Reason’s accident model (and hence also in HFACS) but these not explicitly spelt out. It is not clear in HFACS the mechanism by which categories at higher levels affect categories at lower levels, and ultimately result in active failure (errors) in front line operators even though (as noted earlier) there are strong statistical association in many cases (Tvaranyas, Thompson and Constable, 2006; Li and Harris 2006a; Li and Harris, 2006b; Li, Harris and Yu, 2008).

It is suggested in an Open System, constraints to act can be thought of as existing along a continuum. ‘Hard’ constraints can be defined as physical barriers to prevent certain actions; ‘Firm’ constraints can be characterized by rules and regulations (these can be breached); and ‘Soft’ constraints are typified by social norms and culture. Morley and Harris (2006) noted that required actions (including constraints to act) can also be moderated by other influences and concerns and that these differ at different levels in the organizational (and extra-organizational) hierarchy. In an open system, any constraints can only be at bets, ‘firm’ constraints (e.g. in the form of contractual clauses, quality assurance procedures or regulatory requirements).

Harris and Morley (2006), however, note that some organizations are a great deal more ‘open’ than others. They argue that the operation of military aircraft is a more closed system than is the operation of a civil airline. Military aviation exerts a great deal more control over flight operations and also the context in which it operates (at least in peacetime operations). Not only does it own and operate the aircraft that it flies, it also has a considerable hand in their design, development, maintenance and mid-life updates. Air forces operate their own airfields from which they fly and also provide their own Air Traffic Management/Air Traffic Control (ATM/ATC) services. They train their own pilots and personnel who indoctrinated into the military culture and way of working. In contrast, civil airlines operate into a wide range of airports (none of which they own); maintenance is often provided by third parties and ATM/ATC is provided by the air traffic services providers of the national authorities of the countries which they either operate into or overfly. Furthermore, in the case of the new generation of low-cost carriers they may not even own their own aircraft, employ their own ground and check-in personnel, and in extreme cases, they may not even employ their own pilots.

Limitations of HFACS in Open Systems

It can be seen that there are a great deal more inter-organizational boundaries that information and resources must cross in the operation of commercial aircraft compared to the operation of military aircraft. As will be illustrated in the following case study, accidents in civil aviation are often characterised by errors promulgating across organizational boundaries. It is relatively rare that accidents in civil commercial aviation involve a single organizational entity. However, there is a fundamental assumption inherent in the architecture of HFACS that the root causes of an accident are all internal to the organization. Wiegmann and Shappell (2003) suggest that external influences to the organization all act at via level 4 (Organizational Influences). While this may be true in the operation of military aircraft (organizations which are relatively closed systems) this is certainly not the case in the civil world. Referring back to the opening section of this paper, it will be recalled that HFACS was developed as a military (US naval aviation) human factors accident investigation tool.

Reason's approach to the causation of human error upon which HFACS is based itself also needs to be placed within the historical context in which it was developed. It has already been noted that HFACS was developed within the 'closed' environment of naval aviation but Reason's organizationally-based model of error was also developed during a time when organizations themselves were much more 'closed' than they are today. Reason developed his approach during the 1980s, however the nature of business has changed dramatically during the last two decades (or so). At the beginning of the 21st

century there is a great deal more outsourcing, off-shoreing and sub-contracting of functions previously undertaken within the organization. Reason's model also implicitly assumes a semi-'closed' system.

Clearly, what is required is a simple extension to the HFACS methodology that can account for errors promulgating across organizational boundaries, to accommodate the Open System nature of modern airline operations. What is proposed is essentially a hybrid model for accident analysis extending the HFACS by using many elements and concepts borrowed from the STAMP (Systems-Theoretical Accident Model and Processes) model (Leveson, 2002, 2004).

It has been argued that the principal shortcoming of HFACS is that it was predicated upon a semi-closed system model of aircraft operation, which was appropriate for military operations (during the 1980s) but is not suitable for use in the open system environment found in civil aviation operations. As a result is could not easily incorporate errors which migrated across organizational boundaries. STAMP, on the other hand, has been developed using a systems engineering approach and hence incorporates the involvement of multiple systems through the notion of the control and communication of constraints. In STAMP, accidents are considered to result from inadequate control or enforcement of safety-related constraints (occurring during the design, development or operation of the system) and not from individual or component failures. Leveson proposes that systems are interrelated components kept in a state of dynamic equilibrium by feedback loops of information and control. Safety is a product of control structures embedded in an adaptive socio-technical system. Accidents are viewed as control failures.

STAMP comprises of three basic concepts: hierarchical levels of control, process control models and constraints. All systems are made up of hierarchically-arranged control structures which require effective communication channels in the form of both downward reference channels (providing the information necessary to impose constraints on lower levels in the organizational hierarchy) and upward measurement channels to provide feedback. Process control models require that to control a system four conditions are required (Ashby, 1956): the controller (which may be a person or a function within an organization) must have a system goal; this controller must be able to affect the state of the system; they must have a model of the system, and finally the controller must be able to observe the state of the system. In a complex system, for example an organization such as an airline, there may be several, hierarchically-arranged, control functions (cf. Reason's model of organizationally-based error inherent in the HFACS framework). Safety-related constraints specify the relationships between system variables that constitute safe system states. The control processes enforce these constraints on system behaviour. In an open-system, control processes and constraints also need to be imposed between components in different organizations, for example, between air traffic control and the crew on an aircraft's flight deck.

Leveson (2002, 2004) proposed three basic categories of control flaws (with sub-categories) which may result in accidents. These are outlined in Table 1. Leveson has applied this approach to the analysis of several accidents where multiple agencies were involved (e.g. the shoot down of the Black Hawk helicopters over northern Iraq due to friendly fire - Leveson, Allen and Storey, 2002; the Boeing 757 Cali accident in Columbia – Leveson, 2004; and the loss of the Ariane 5 Launch vehicle – Leveson, 2002).

INSERT TABLE 1 ABOUT HERE

However, the human factors element of STAMP is somewhat limited and under-specified. Human error is conceptualised as essentially a failure of the operator's mental model of the system and although Leveson acknowledges the pivotal role of the managerial aspects in a socio-technical system, these managerial and social issues within an organization are simply regarded as sources of failure in control constraints. The model of human behaviour implicit in STAMP is somewhat deterministic. However, by combining the categories and structure from HFACS with its underlying mechanisms describing the contributory factors to error, with the elements of STAMP that specify the nature (and failures) of the system constraints in an accident, a more complete analysis of the contributing factors and their inter-relationships, may be arrived at.

HFACS-X (Extended)

HFACS-X is a simple extension to the basic HFACS approach incorporating the control and constraint concepts from STAMP, and also incorporating the Open Systems concepts inherent in the latter model.

HFACS-X commences with a basic HFACS analysis, however each organization (or sub-unit within an organization) implicated in the accident causal sequence is subject to an individual HFACS analysis. In HFACS-X all errors are transmitted from one organization to another via an active failure of an operator (level 1: 'Unsafe Acts'). However, unlike the model proposed by Weigmann and Shappell (2003) they may be received into another organization at any level in the HFACS hierarchy (not just at the top level – level 4: 'Organizational Influences'). Furthermore, as the promulgation of errors across organizations requires communication (this is an open systems approach) the nature of this communication shortfall can be also be characterised according the Levenson's categories of control flaws. Furthermore, for the HFACS analyses conducted within each organization in HFACS-X the linkages between categories are also characterized using STAMP control flaws taxonomy.

The operation of HFACS-X is described using the following case study from the Uberlingen mid-air collision on 1 July 2002 (Bundesstelle für Flugundfalluntersuchung - BFU, 2004).

The Accident

The accident involved two aircraft, Bashkirian Airlines flight BTC 2937, a Tupolev Tu-154M and DHL flight DHX 611, a Boeing 757-200 freighter, at approximately 22:35 (local). The two aircraft were both flying at flight level 360 (approximately 36,000 feet) in airspace controlled from the Zurich Air Traffic Control Centre (ATCC). Very shortly before the collision (less than one minute) the air traffic controller on duty noted that the two aircraft were occupying the same flight level and were on converging courses. He contacted the crew of the Tupolev Tu-154M and instructed them to expedite a descent to avoid the conflicting traffic. However, shortly after initiating the avoiding action, the Traffic Collision Avoidance System (TCAS) on the Russian aircraft's flight deck issued a RA (Resolution Advisory) instructing them to *climb*. The pilots on board the Tupolev disregarded this TCAS directive and followed the instructions issued from the Zurich ATCC. Simultaneously, the TCAS in the DHL Boeing 757-200 instructed the pilots to descend. They followed the TCAS RA but could not contact Zurich ATCC to inform the controller due as he was dealing with the Bashkirian Airlines flight. Both aircraft were now descending on converging tracks.

In Zurich ATCC (operated by Skyguide, a company providing air traffic control services for Switzerland) there was only one controller on duty, working two positions simultaneously, one of which was controlling the airspace in which the two aircraft were flying. There was another other controller on duty but (contrary to regulations) he was resting in another room. This was a common practice during quiet periods at night and was known and tacitly tolerated by the management. There was also maintenance work being undertaken on the ATCC's systems at the time. As a result of a re-definition of the upper airspace sectorisation being undertaken, which involved various systems being updated, some facilities normally available to controllers were not operational. These included the radar processing and presentation system and the multi-radar processing computer. As a result, there was no automatic correlation of flight plan data with radar image data. The visual representation of the Short Term Conflict Alert (STCA) systems at the controller's workstation was also not operational (the auditory warning was still operational, though). The visual system operated to give a 120 second warning prior to the aircraft coming within 6.5 nautical miles of each other. The auditory system operated below 6.5 miles separation. Owing to the system updates being undertaken there was both a stand-by controller and a system manager on call but at no point were these called upon at any time.

The main (fixed) telephone lines between adjacent ATCCs were also inoperative as a result of the system updates taking place and unfortunately the backup line (which used the public telephone system) was also defective. Shortly before noticing the impending conflict, the controller handling the airspace was also working a delayed flight into Friedrichshafen Airport but was having difficulty handing off the aircraft to the approach controller as a result of the malfunctioning telephone system. The malfunctioning 'phones also prevented controllers in the adjacent sector at from telephoning in a warning. As the controller was working an Airbus A320 into Friedrichshafen he was also operating on a different frequency to the two aircraft transitioning his airspace and as a result he missed several radio calls.

Zurich ATCC was also unaware of the TCAS advisories issued on each flight deck. The controller repeated his instruction to the Tupolev Tu-154M to descend while also simultaneously passing incorrect information concerning the position of the DHL Boeing 757-200 (it was reported as being above the Tupolev 154M and at its 2 o'clock position instead its actual position at its 10 o'clock). This caused some confusion on the Russian aircraft's flight deck. As a result of the transmissions between Zurich centre and the Bashkirian Airlines aircraft, the crew of the DHL Boeing 757 was unable to inform the controller that they were descending in response to a TCAS RA. Once the controller had finished his transmission to the Tupolev, he returned his attention to the Airbus A320 he was working into Friedrichshafen.

The auditory short term conflict alert triggered 32 seconds before the collision but was not heard by anyone in Zurich ATCC. Subsequently, the two aircraft collided at almost right angles at an altitude of 34,890 feet. Sixty-nine people on board the Tupolev and two on board the Boeing were killed.

The main findings of the accident report were as follows:

> *The following immediate causes have been identified: (1) The imminent separation infringement was not noticed by ATC in time. The instruction for the TU154M to*

descend was given at a time when the prescribed separation to the B757-200 could not be ensured anymore; (2) The TU154M crew followed the ATC instruction to descend and continued to do so even after TCAS advised them to climb. This manoeuvre was performed contrary to the generated TCAS RA.

The following systemic causes have been identified: (1) The integration of ACAS/TCAS II into the system aviation was insufficient and did not correspond in all points with the system philosophy. The regulations concerning ACAS/TCAS published by ICAO and as a result the regulations of national aviation authorities, operations and procedural instructions of the TCAS manufacturer and the operators were not standardised, incomplete and partially contradictory; (2) Management and quality assurance of the air navigation service company did not ensure that during the night all open workstations were continuously staffed by controllers; (3) Management and quality assurance of the air navigation service company tolerated for years that during times of low traffic flow at night only one controller worked and the other one retired to rest.

Bundesstelle für Flugundfalluntersuchung (2004). Investigation Report AX001-1-2/02. Braunschweig: Author. p.112

It was also established there were key differences between the rules covering the right of way of aircraft between Western European/North American nations and those implemented in the Russian Federation. Western European/North American rules required the aircraft on the left to give way. The aircraft on the right should maintain its course and altitude and the other aircraft should manoeuvre safely around it. The rules of the Russian Federation, though, require the left hand aircraft of the pair to descend (as in the case of the Tupelov) and the right hand aircraft to climb. However, when in receipt of a TCAS RA, ICAO (International Civil Aviation Organization) procedures require that these instructions should take precedence (and in this case the controller is absolved of the responsibility to maintain safe separation until the conflict is resolved).

Analysis using HFACS-X

Two within-organization analyses are presented using HFACS-X describing the actions and influences in both the Zurich ATCC operated by Skyguide and within Bashkirian Airlines, including the Tupolev Tu-154M flight deck. No HFACS-X analysis is presented for the DHL Boeing 757-200 as the crew of this aircraft committed no significant errors and were essentially innocent victims of events. However, the DHL aircraft is represented as an element external to both the Skyguide operation and the Tupelov flight deck which had some part to play. This also applies to the adjacent Karlsruhe ATCC. Also represented are the ICAO and the Russian Federation, as these regulatory authorities were responsible for producing slightly conflicting rule sets (regulatory 'firm' constraints) that were implicated in the sequence of events. As a result, the HFACS-X analysis commences with a representation of how the errors or lack of control of constraints promulgated across the organizations involved (see Figure 2).

INSERT FIGURE 2 ABOUT HERE

The major failure proximal to the accident in the Uberlingen mid-air collision was a failure of the Skyguide air traffic controller in Zurich ATCC to notice in a timely manner that two aircraft were on converging courses at the same flight level. This error was then promulgated across organizations and compounded when Zurich ATCC gave incorrect positional information concerning the conflicting DHL Boeing 757 to the crew on the Bashkirian Airlines Tupolev Tu-154M flight deck when they expedited their descent. The controller also failed to notice that the Boeing 757 had also initiated a descent in response to a TCAS advisory, as being the only controller on duty he was overloaded because he was simultaneously trying to coordinate the approach of an Airbus A320 into Friedrichshafen airport.

The error made by the controller, which in HFACS terms may be categorized as both a 'Skill-Based Error' (failure to see and avoid; failure to prioritize attention; task overload – see Wiegmann and Shappell, 2003) and a 'Decision Error' (inappropriate manoeuvre/procedure; wrong response to emergency) resulted in a firm constraint being broken (Checkland, 1981) specifically the safe separation minima between aircraft. In terms of Leveson's (2002, 2004) STAMP model this was as a result of an 'Inadequate Control Action' (enforcement of constraints), specifically an inappropriate, ineffective or missing control action (see Table 1). This was followed by 'Inadequate Execution of a

Control Action' (both in terms of a communication flaw and a time lag) and there was also 'Inadequate or Missing Feedback' about the failure to resolve the conflict. This may be regarded as a product of poor system design (assuming that the short term conflict alert did not sound or was not heard) but also the controller failed to perceive the result of their actions as their attention was turned away towards other matters.

The result of this controller error was that the crew of the Tupolev were initially unaware of the conflicting aircraft (at HFACS level 2: 'Preconditions for Unsafe Acts' this would be categorized as a loss of situational awareness which falls within the sub-category of 'Adverse Mental State'). This was then compounded by the controller subsequently informing them of the incorrect relative bearing to the conflicting Boeing, which seemed to further erode their situation awareness while simultaneously generating some indecision and discussion on the flight deck, symptomatic of poor 'Crew Resource Management' (CRM), a further HFACS level 2 category (see Figure 1). Thus is can be demonstrated that the influence of the actions from another organization exerted themselves not at HFACS level 4 (as proposed by Weigmann and Shappell, 2003) but much closer to the operation of the aircraft.

It can also be seen that in Figure 2 the indirect control processes enforcing the separation constraints between the Karlsruhe ATCC, Zurich ATCC and the DHL Boeing 757 are described as being 'inhibited'. The attempts by the adjacent ATCC to notify Zurich ATCC of the impending loss of separation were unsuccessful ('Inadequate or Missing Feedback' as a result of a communication flaw – i.e. the serviceability of the telephone lines as a result of the system upgrades being undertaken). Simultaneously, attempts by the crew of the Boeing 757 to notify Zurich ATCC that they were *descending* in response to a TCAS RA were inhibited as a result of the controller repeating his instruction to the Tupolev Tu-154M to descend while simultaneously passing incorrect information about the position of the DHL Boeing 757-200. Furthermore, the crew of the Russian aircraft would not have been aware of the Boeing's actions (as they would normally have been from listening in on the transmissions of other aircraft sharing their sector) as the DHL crew was unable to make the transmission (using the control flaw categories from the STAMP model, this was 'Inadequate or Missing Feedback', specifically a communication flaw – see Table 1).

There was also a conflict in the constraints on behaviour imposed by the ICAO and by the Russian Federation in the appropriate manner in which to respond to conflicting traffic (Figure 2). This manifested itself in *inappropriate* avoiding action being taken by the Tupolev crew, in the context of German airspace. In terms of the STAMP model, this was an 'Inadequate Control Action' (enforcement of constraint) specifically as a result of an inconsistent process model – see Table 1. This conflict in the control constraints acted at HFACS level 3 in Bashkirian Airlines, in the form of 'Inadequate Supervision'. In the HFACS framework described by Weigmann and Shappell (2003) inadequate training falls into this category, and it would seem that the Russian Crew were inadequately trained in the operation of TCAS and the procedure to follow in the presence of conflicting traffic when outside Russian Airspace (BFU, 2004). Furthermore, the crew has no previous experience of such a situation, which HFACS classifies as falling within the category of a ‘Physical/Mental Limitation’ at level 2 (see Figure 2). Once the crew had made the incorrect decision to descend, rather than follow the TCAS advisory (an error at HFACS level 1) the crew of the DHL aircraft subsequently became the innocent victim of their error.

Zurich ATCC (Skyguide) HFACS-X Analysis

Within Skyguide the management had tacitly condoned the practice of allowing only a single controller to be on duty during off-peak periods (an issue with the ‘Organizational Climate’ within Skyguide – HFACS level 4 - leading to ‘Inadequate Supervision’ and ‘Supervisory Violations’ at level 3). Using the control flaws sub-categories from STAMP this can be regarded as an ‘Inadequate Control Action’ (enforcement of constraints) and specifically inappropriate, ineffective or missing control actions and a control process that did not enforce constraints (see Table 1). Enhancements to the safety culture within the organization were taking place at the time of the accident, however the programme had not been rolled out fully across the organization. There was poor coordination of the update work revising the sectorisation of the airspace and the implications that it would have on the serviceability of equipment. This failure to coordinate was a result of poor ‘Organizational Processes’ at HFACS level 4 leading to ‘Planned Inappropriate Operations’, via the control flaw category of ‘Inadequate Control Actions’ (enforcement of constraints), specifically an inappropriate, ineffective or missing control actions for identified hazards. This also led to compromises in the availability of key features of the air traffic control equipment (e.g. the short term conflict alert and no automatic correlation of flight plan data with radar image data) which is characterized by the ‘Inadequate Execution of Control Actions’ (specifically inadequate actuator operations) leading to a compromise in the ‘Technology Environment’ (HFACS level 2).

INSERT FIGURE 3 ABOUT HERE

The inadequate supervision within the Zurich ATCC manifested itself in several ways but most specifically, the lack of oversight and a failure to track performance subsequently resulted in the controller becoming overloaded (‘Physical/Mental Limitation’) and losing his awareness of the developing traffic situation (‘Adverse Mental State’). The HFACS ‘Supervisory Violation’ in the form of failing to enforce operating rules also served to the same ends. The firm control constraints leading to these psychological pre-cursors of unsafe acts were all eroded as a result of what are classified in the STAMP model as inadequate execution of control actions. All the required control actions were potentially present in the Skyguide organization, however they were not executed to the standard required. The continuance of ‘normal’ operations at Zurich ATCC (including the routine, tacitly approved de-manning of the control centre during quiet periods) while the upgrade work was being undertaken was certainly a ‘Planned Inappropriate Operation’. The fact that additional staff were available (a stand-by controller and a system manager were on call) again points to appropriate control actions being in place but again were not executed to the standard required.

The inadequacies in the 'Technological Environment' (HFACS level 2) as a result of the system upgrades resulting in no visual STCA and poor quality telephone lines to communicate with adjoining sectors resulted in the 'Perceptual Error' of the controller failing the notice that the two aircraft remained on a collision course after he had taken the initial actions to resolve the conflict. In the STAMP model this can be characterized as a form of 'Inadequate or Missing Feedback' (Figure 3).

Bashkirian Airlines (including the Tupolev Tu-154M flight deck) HFACS-X Analysis

Bashkirian Airlines did not have a simulator equipped with TCAS, so as a result the Russian crew had no practical experience of responding to a RA. TCAS was not a mandatory fit for aircraft operating within the Russian Federation. It was only a requirement for aircraft operating in Western European/North American airspace. Furthermore, the crew had also not undertaken any computer-based training addressing the interpretation of a TCAS display and the correct procedures to be applied for responding to an RA. The crew had, however, undertaken TCAS training at an approved Russian 'State Special Centre' which involved a lecture course on the operation of TCAS and the procedures to be followed. Flight deck familiarisation with the TCAS equipment had also taken place. However the BFU concluded that the level and nature of the training undertaken by the Tupolev crew was a significant factor in causing the collision

(BFU, 2004). CRM training within Bashkirian Airlines was also criticised by the BFU on a similar basis, particularly the absence of LOFT (Line Orientated Flight Training) which gave the crew the opportunity to practice the theoretical aspects of the training received. The CRM training was, however, being improved at the time of the accident. Within the HFACS framework, inadequate training falls within the level 3 category of ‘Inadequate Supervision’ (see Weigmann and Shappell, 2003). Using the classification of control flaws from the STAMP model (Leveson, 2002; 2004) this lack of adequate training resulted in an ‘Inadequate Execution of a Control Action’ (specifically, inappropriate communication of the TCAS system operation and constraints) which led to poor CRM at HFACS level 2 and a ‘Physical/Mental Limitation’ (specifically the lack of necessary experience to deal with the complexity of the situation). However, very few flights were undertaken by the airline outside of Russia, so a further factor was the relative inexperience of the crew with the operating rules in German airspace, but given that so few flights were undertaken by the airline outside Russian Federation airspace it would seem somewhat harsh to criticise the higher levels of the company (at HFACS level 4) for failing to provide these simulator facilities (an issue in ‘Resource Management’). However, this link (an ‘Inadequate Control Action’) is included for completeness (see Figure 4).

INSERT FIGURE 4 ABOUT HERE

On the flight deck of the Tupolev evidence from the Cockpit Voice Recorder suggests a breakdown in CRM as a result of the conflicting requirements from the TCAS system (to climb) and Zurich ATCC (to descend). As noted previously, this failure in CRM was partly attributable to training inadequacies. The Captain elected to follow the instructions of the controller, which would have been compatible with Russian Federation collision avoidance procedures but conflicted with TCAS procedures (which should override air traffic control instructions in the advent of an RA). The First officer was uncomfortable with this decision and questioned the decision twice (after the initial decision and subsequently after the TCAS issued a further, urgent RA to climb). However, his comments were not made forcefully enough for the Captain to reverse his decision to follow the controller's instructions. This HFACS level 2 failure in 'CRM' and the 'Physical/Mental Limitation' also resulting from a lack of experience as a result of the manner in which the training had been performed directly led to the inappropriate decision to descend the aircraft (HFACS level 1 'Decision Error'). A further HFACS level 2 component, the 'Adverse Mental State' (specifically a lack of situation awareness resulting from the error in Zurich ATCC) also contributed to the ultimate decision by the Captain to descend the aircraft instead of following the TCAS RA.

Discussion

Characterising the mechanisms connecting the organizational structures in the HFACS-X model as control mechanisms enforcing safety constraints allows a further degree of explanatory power to be leveraged over and above that of the original HFACS approach Wiegmann and Shappell, 1997, 2001a, 2001b, 2001c, 2003; Shappell and Wiegmann 2001, 2003, 2004). Although statistical associations between the HFACS levels and categories had been established in previous research (Tvaranyas, Thompson and Constable, 2006); Li and Harris 2006a; Li and Harris, 2006b; Li, Harris and Yu, 2008) characterising failures in these constraint control procedures using the classification of control flaws from the STAMP model (Leveson, 2002, 2004) helps explain the nature of the mechanisms of failure. Furthermore, it also provides a suitable mechanism to describe how failures in one organization may be transmitted to another organization, something that was missing in the original HFACS framework. This is essential to understand accident processes in open systems, such as the air transport system.

The application of control flaws to describe the nature of failures between the components in the HFACS-X model is of greatest utility when considering the routes to failure between levels 4 and 3 (Organizational Influences to Unsafe Supervision), and levels 3 and 2 (Unsafe Supervision to Preconditions for Unsafe Acts). In these cases the control constraint mechanisms (and hence control flaws) can more readily be understood, interpreted and ultimately remediated, as the paths described lie between organizational processes/entities to ultimately produce an effect on the operator at the ‘sharp end’. The control paths between levels 2 and 1 (Preconditions for Unsafe Acts to Unsafe Acts) lie internally within the operator at the ‘sharp end’. As a result, the control constraint mechanisms and control failures are less easy to specify. The Preconditions for Unsafe Acts are essentially what Reason (1990) describes as the Psychological Precursors to the active failures that an operator makes (the errors proximal to the accident). The paths between categories in levels 4, 3 and 2 are associated with the systemic (latent) failures distal failures lying dormant within a system.

It can also be seen from the Uberlingen case study that issues external to a particular organization can exert their influence at levels other than HFACS level 4. Indeed, in the Uberlingen accident the influence of errors made in Zurich ATCC was mostly at HFACS level 2 in the cockpit of the Tupolev, inhibiting the development of good situation awareness and encouraging poor CRM. The STAMP control flaw categories provide a useful mechanism for networking individual, intra-organization HFACS analyses into a system-wide analysis of an accident.

It has been demonstrated that coding accidents using the HFACS system can be undertaken reliably (Gaur, 2005; Li and Harris, 2005) however the inter-rater reliability of the coding of the categories of control flaws derived from the STAMP approach proposed by Leveson (2002, 2004) needs to be established. It also needs to be established that the extended HFACS approach proposed in this paper can be applied meaningfully to more complex analyses involving many more organizations in the accident causal sequence.

It was suggested that the HFACS framework confounds categorization and analysis Dekker (2001). Leveson herself also has suggested that the human error component with STAMP model is somewhat underspecified (Leveson, 2002). It is suggested that the hybrid analytical procedure described here (HFACS-X) combining the features of HFACS and STAMP, produces a system with enhanced explanatory power which addresses the shortcomings of both previous systems.

References

AERONAUTICA CIVIL OF THE REPUBLIC OF COLOMBIA 1995. *Controlled Flight into Terrain: American Airlines Flight 965, Final Report of Aircraft Accident: American Airlines Flight 965, Boeing 757-223, N651AA near Cali, Colombia, December 20, 1995* (Santafe De Bogota, D.C., Colombia: Author).

ANDRES, D.M., LUXHØJ, J.T. and COIT, D.W. 2005, Modelling of human-system risk and safety: aviation case studies as exemplars. *Human Factors and Aerospace Safety*, **5**, 137-168.

ASHBY, W.R. 1956, An *Introduction to Cybernetics* (London: Chapman and Hall).

BAKER, S. 1995, Putting ‘human error’ into perspective. *Aviation, Space and Environmental Medicine*, **66**, *521*.

BEAUBIEN, J.M., and BAKER, D.P., 2002, A Review of Selected Aviation Human Factors Taxonomies, Accident/Incident Reporting Systems and Data Collection Tools. *International Journal of Applied Aviation Studies*, **2**, 11-36.

BENNER, L. 1975, Accident investigation: Multilinear events sequencing methods. *Journal of Safety Research*, **7**, 6-73.

BUNDESSTELLE FÜR FLUGUNDFALLUNTERSUCHUNG, 2004, *Investigation Report AX001-1-2/02* . (Braunschweig: Author).

CHECKLAND, P. 1981, *Systems Thinking, Systems Practice* (New York: John Wiley and Sons).

DEKKER, S.W.A., 2001. The re-invention of human error. *Human Factors and Aerospace Safety*, **1**, 247-266.

DIEHL, A., 1989. Human Performance/System Safety Issues in Aircraft Accident Investigation and Prevention, in *Proceedings of 11th International Symposium on Aviation Psychology* (Columbus, OH: Ohio State University Press).

GAUR, D., 2005. Human Factors Analysis and Classification System Applied to Civil Aircraft Accidents in India. *Aviation, Space, and Environmental Medicine.* **76**, 501-5.

HARRIS, D. and MORLEY, F.J.J. 2006, Keynote Address: An Open Systems Approach to Safety Culture: Actions, Influences and Concerns, in *Proceedings of the Australian Aviation Psychology Association (AAvPA) International Conference – Evolving System Safety 2006.* Sydney, Australia 9-12 November (Sydney: Australian Aviation Psychology Association).

HENDRICK, K. and BENNER, L. 1987, Investigating Accidents with Sequentially Timed and Events Plotting (STEP) (New York, NY: Marcel Decker).

JENSEN, R.S., 1997, The Boundaries of Aviation Psychology, Human Factors, Aeronautical Decision Making, Situation Awareness, and Crew Resource Management. *International Journal of Aviation Psychology* **7**, 259-68.

KATZ, D. and KAHN, R.L. 1978, *The Social Psychology of Organizations (2nd Edition)* (New York: Wiley).

KRULAK., D.C., 2004, Human Factors in maintenance: Impact on aircraft mishap frequency and severity. *Aviation, Space, and Environmental Medicine.* **75**, 429-432.

LECHNER, K.W. and LUXHØJ, J.T. 2005, Probabilistic causal modelling of risk factors contributing to runway collisions: case studies. *Human Factors and Aerospace Safety*, **5**, 185-216.

LENNÉ, M. 2006, Enhancing the collection and analysis of general aviation insurance data, in *Proceedings of the Australian Aviation Psychology Association (AAvPA) International Conference – Evolving System Safety 2006.* Sydney, Australia 9-12 November (Sydney: Australian Aviation Psychology Association).

LENNÉ, M.G., ASHBY, K. and FITZHARRIS, M. 2008. Analysis of General Aviation Crashes in Australia Using the Human Factors Analysis and Classification System. *International Journal of Aviation Psychology,* **18**, 340-352.

LEVESON N. 2004, A New Accident Model for Engineering Safer Systems. *Safety Science,* **42**, 237-270.

LEVESON, N. 2002, *A New Approach to System Safety Engineering* (Cambridge, MA. MIT).

LEVESON, N.G., Allen, P. and Storey, M.A. 2002, The Analysis of a Friendly Fire Accident using a Systems Model of Accidents, in *Proceedings of the 20th International System Safety Conference*, Denver, Colorado, 5-9 August 2002 (Denver, CO: International System Safety Society).

LI, W.C., and HARRIS, D. 2005, HFACS Analysis of ROC Air Force Aviation Accidents: reliability analysis and cross-cultural comparison. *International Journal of Applied Aviation Studies*, **5**, 65-81.

LI, W.C., and HARRIS, D. 2006a, Pilot error and its relationship with higher organizational levels: HFACS analysis of 523 accidents. *Aviation, Space, and Environmental Medicine*, **77,** 1056-1061.

LI, W.C., and HARRIS, D., 2006b, Breaking the Chain: An Empirical Analysis of Accident Causal Factors by Human Factors Analysis and Classification System (HFACS), *in Proceedings of International Society of Air Safety Investigators Seminar 2006*. September 11–14 (Sterling, VA: International Society of Air Safety Investigators).

LI, W-C., HARRIS, D. and YU, C-S. 2008, Routes to failure: Analysis of 41 civil aviation accidents from the Republic of China using the human factors analysis and classification system. *Accident Analysis and Prevention*, **40,** 426-434.

LUXHØJ, J.T. and HADJIMICHAEL, M. 2006, A hybrid fuzzy-belief network (HFBN) for modelling aviation safety risk factors. *Human Factors and Aerospace Safety,* **6**, 191-216.

MORLEY, F.J.J. and HARRIS, D. 2006, Ripples in a Pond: An Open System Model of the Evolution of Safety Culture. *International Journal of Occupational Safety and Ergonomics*, **12**, 3-15.

REASON, J.T., 1990, *Human Error* (Cambridge University Press: Cambridge).

REASON, J.T., 1997, *Managing the Risks of Organizational Accidents* (Aldershot: Ashgate).

REINACH, S. and VIALE, A. 2006, Application of a human error framework to conduct train accident/incident investigations. *Aviation, Space, and Environmental Medicine,* 30, 396-406.

SCHEIN, E.H. 1992, *Organizational Culture and Leadership, (2nd Edition)* (San Francisco, CA: Jossey-Bass).

SHAPPELL, S., DETWILER, C., HOLCOMB, K., HACKWORTH, C., BOQUET, A. and WIEGMANN, D.A. 2007, Human Error and Commercial Aviation Accidents: An Analysis Using the Human Factors Analysis and Classification System. *Human Factors*, **49**, 227–242.

SHAPPELL, S.A., and WIEGMANN, D.A., 2001, Applying Reason: the Human Factors Analysis and Classification System (HFACS). *Human Factors and Aerospace Safety* **1**, 59-86.

SHAPPELL, S.A., and WIEGMANN, D.A., 2003, *A Human Error Analysis of General Aviation Controlled Flight Into Terrain Accidents Occurring Between 1990-1998, Report no. DOT/FAA/AM-03/4* (Washington, DC: Federal Aviation Administration).

SHAPPELL, S.A., and WIEGMANN, D.A., 2004, HFACS Analysis of Military and Civilian Aviation Accidents: A North American Comparison, in *Proceedings of International Society of Air Safety Investigators, Australia, Queensland, 2-8 November, 2004* (Sterling, VA: International Society of Air Safety Investigators).

TVARNYAS, A.P., THOMPSON, W.T., and CONSTABLE, S.H., 2006, Human factors in remotely piloted aircraft operations: HFACS analysis of 221 mishaps over 10 years. *Aviation, Space, and Environmental Medicine*, **77**, 724-732.

VON BERTHALANFRY L. 1956, General systems theory: general systems. *Yearbook of the Society of General Systems Theory*, **1**, 1-10.

WIEGMANN, D.A., and SHAPPELL, S.A., 1997, Human Factors Analysis of Postaccident Data: Applying Theoretical Taxonomies of Human Error. *International Journal of Aviation Psychology,* **7,** 67-81.

WIEGMANN, D.A., and SHAPPELL, S.A., 2001a, Human Error Analysis of Commercial Aviation Accidents: Application of the Human Factors Analysis and Classification System. *Aviation, Space and Environmental Medicine*, **72**, 1006-1016.

WIEGMANN, D.A., and SHAPPELL, S.A., 2001b, Applying the Human Factors Analysis and Classification System to the Analysis of Commercial Aviation Accident Data, in *Proceedings of 11th International Symposium on Aviation Psychology* (Columbus, OH: Ohio State University).

WIEGMANN, D.A., and SHAPPELL, S.A., 2001c, Human Error Perspectives in Aviation. *International Journal of Aviation Psychology*, **11**, 341-357.

WIEGMANN, D.A., and SHAPPELL, S.A., 2003, *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System* (Aldershot: Ashgate).

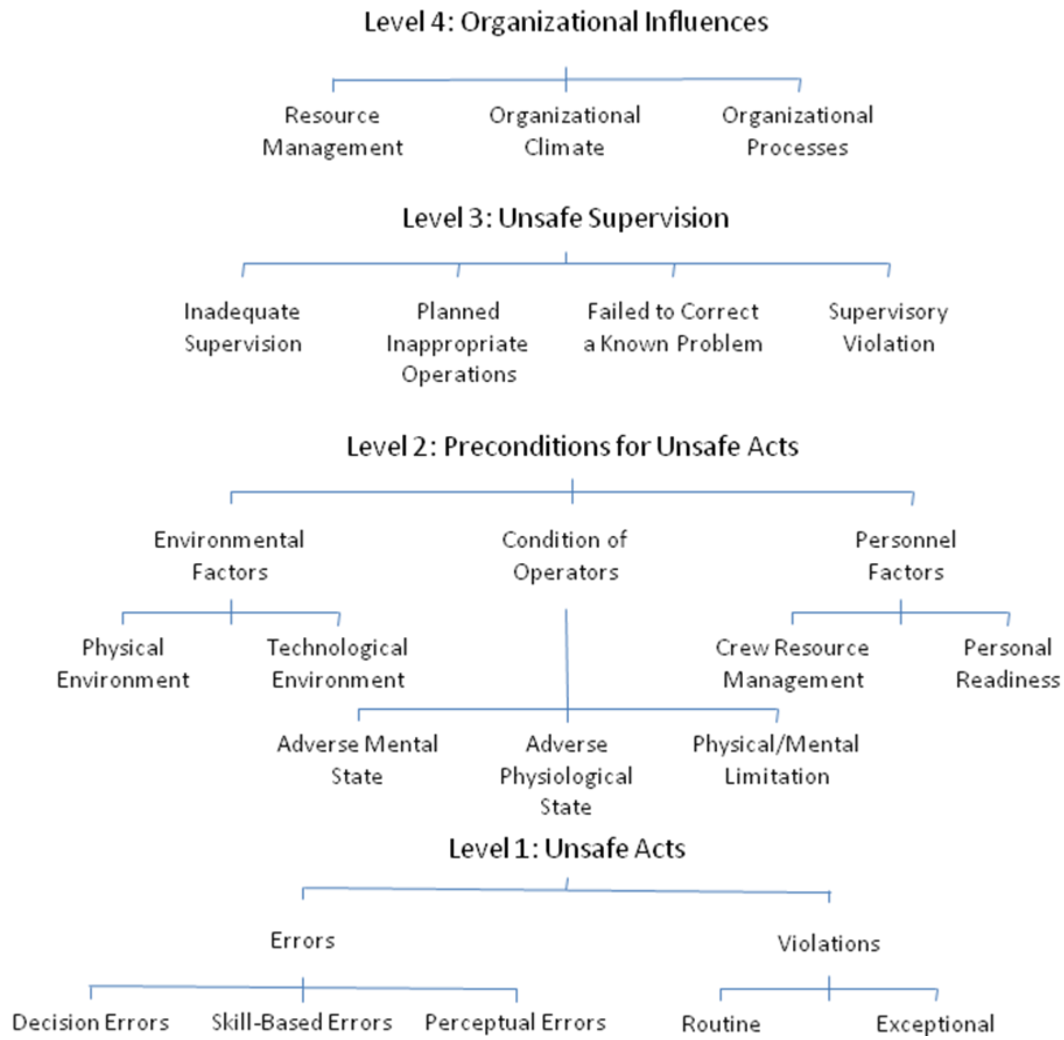

Figure 1 **The HFACS framework. Each upper level is proposed to affect items at the lower levels (Shappell, Detweiler, Holcomb, Hackworth, Boquet and Weigmann, 2007).**

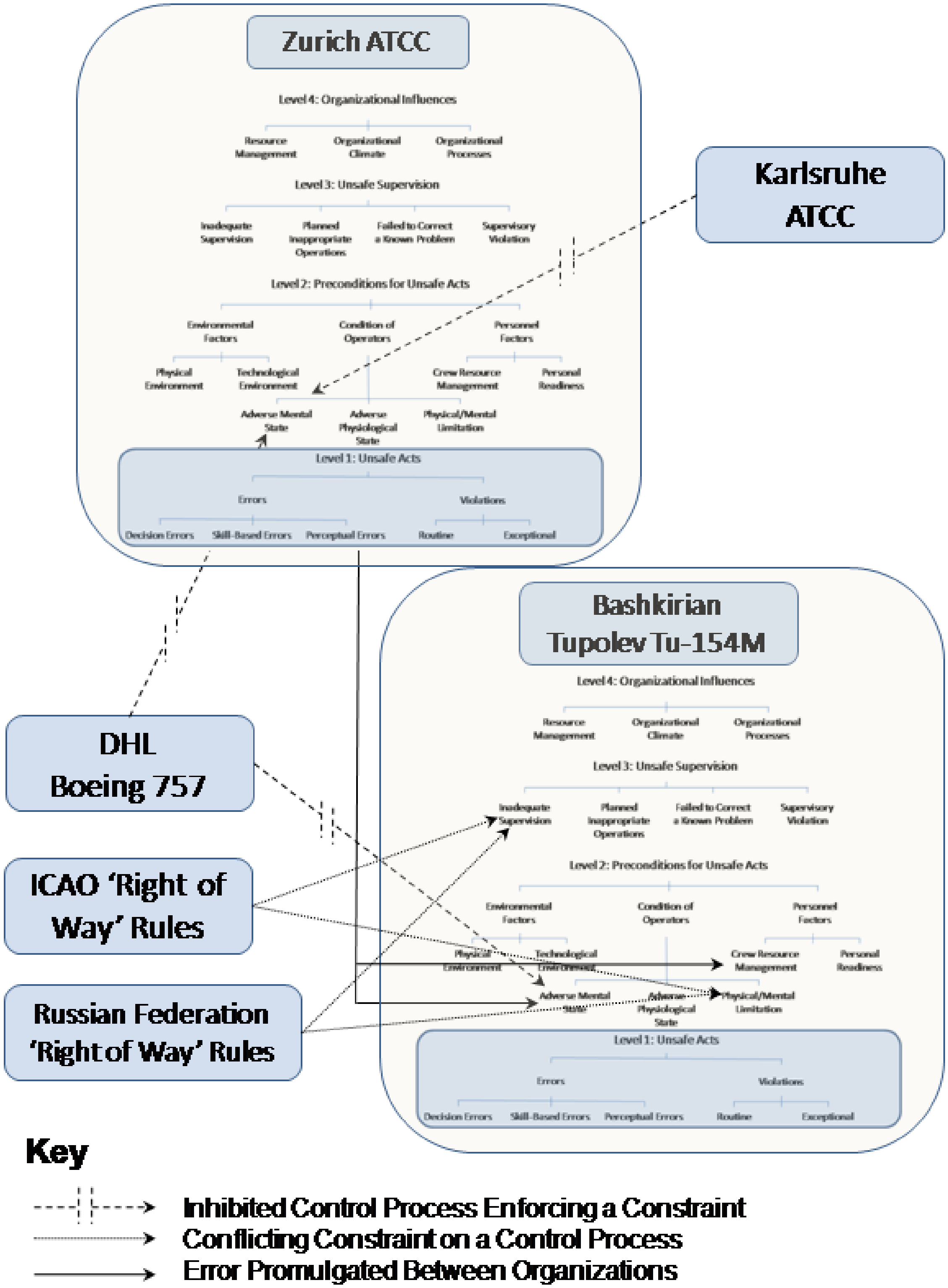

Figure 2 High-level HFACS-X describing the promulgation of errors and the inhibition of constraints between the organizations involved in the Uberlingen mid-air collision.

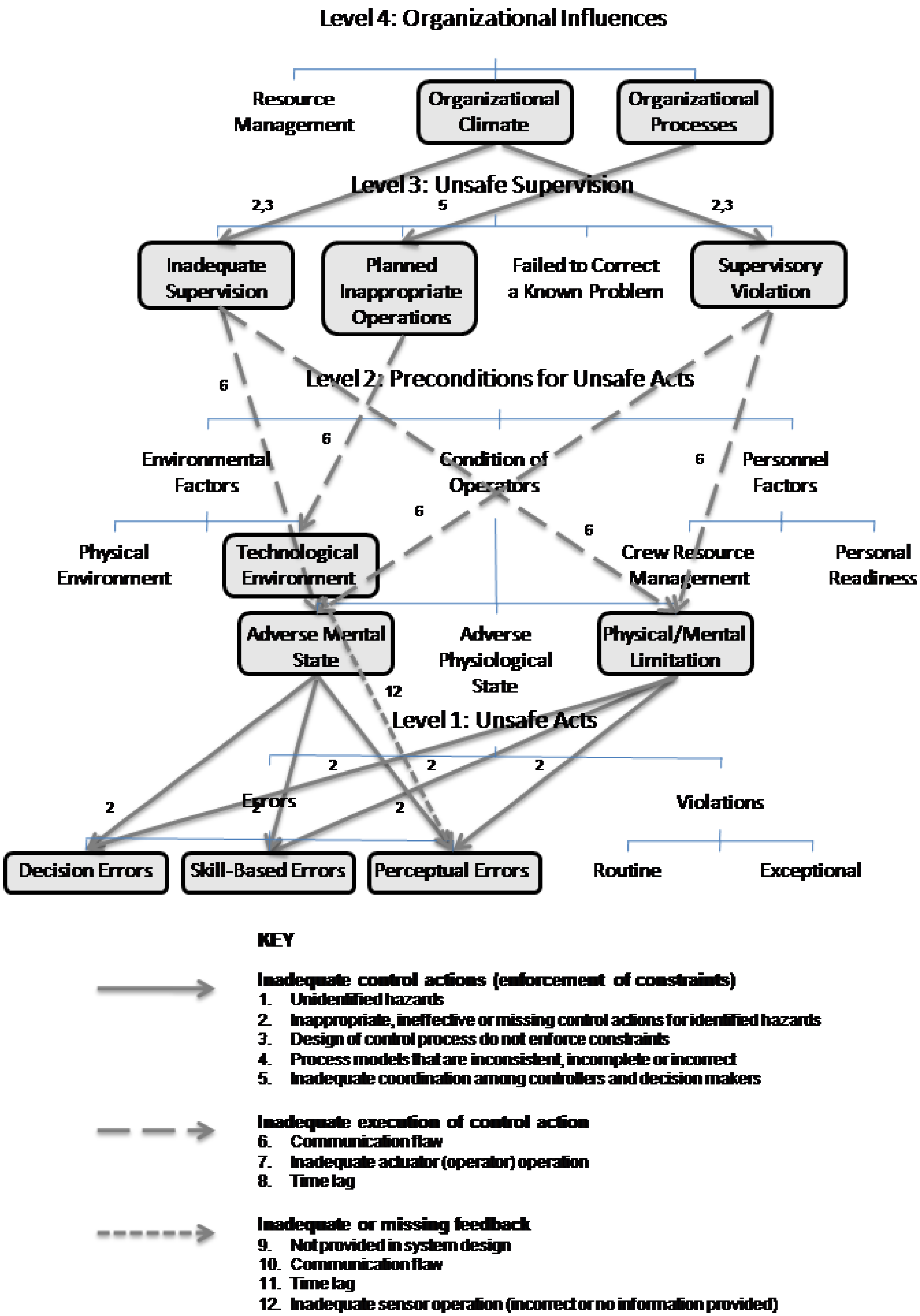

Figure 3 HFACS-X analyses of errors and control mechanism flaws within Skyguide prior to the Uberlingen accident. The numbers on the arrows provide a description of the control flaw category.

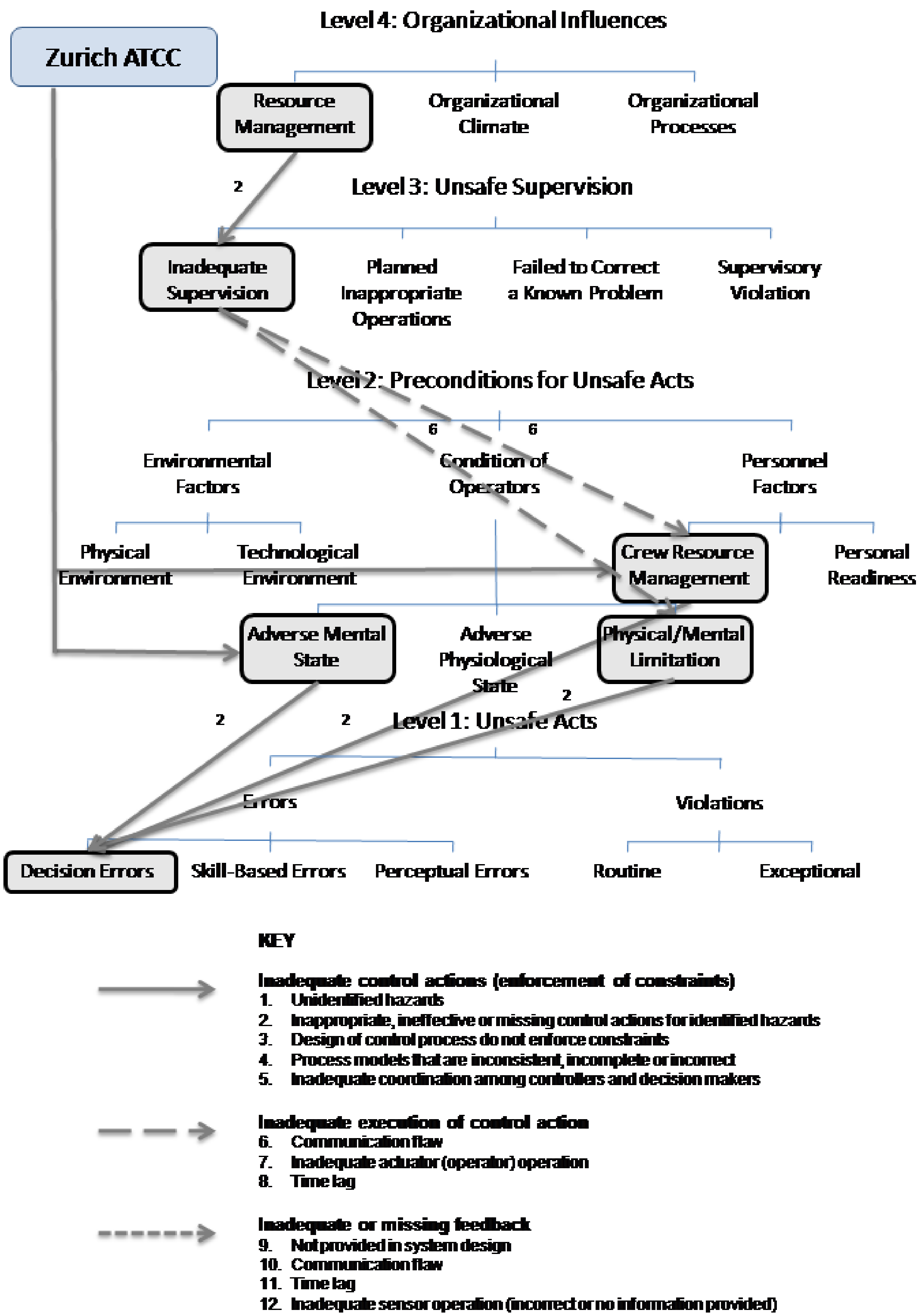

Figure 4 HFACS-X analyses of errors and control mechanism flaws within Bashkirian Airlines (including the Tupolev Tu-154M flight deck) prior to the Uberlingen accident. The numbers on the arrows provide a description of the control flaw category.

Table 1 Leveson's three basic categories of control flaws (with sub-categories)

Inadequate control actions (enforcement of constraints)
Unidentified hazards Inappropriate, ineffective or missing control actions for identified hazards Design of control process do not enforce constraints Process models that are inconsistent, incomplete or incorrect Inadequate coordination among controllers and decision makers
Inadequate execution of control action
Communication flaw Inadequate actuator (operator) operation Time lag
Inadequate or missing feedback
Not provided in system design Communication flaw Time lag Inadequate sensor operation (incorrect or no information provided)