Rule Fragmentation in the Airworthiness Regulations: A Human Factors Perspective

Don Harris

HFI Solutions Ltd., Bradgate Road,
Bedford, MK40 3DE, United Kingdom
`don.harris@hfisolutions.co.uk`

Abstract. Human error has been identified as the primary risk to flight safety. Two of the more pervasive aspects of Human Factors encountered throughout the airworthiness regulations are error and workload. However, as a result of increasing organizational inter-dependence and integration of aircraft systems it is argued that the manner in which these issues are addressed in the aviation regulations is becoming increasingly incompatible with human and organizational behavior in an airline. Workload and error are both products of complex interactions between equipment design, procedures, training and the environment. These issues cannot be regulated on a localized basis. A more systemic, holistic approach to Human Factors regulation is required. It is suggested that a Safety Case-based approach may be better used as an adjunct to existing regulations for Human Factors issues.

Keywords: Regulations, Workload, Error, Accidents, Socio-technical systems, Safety Case.

1 Introduction

For the last decade the serious aircraft accident rate has remained relatively constant at approximately one per million departures [1]. However, as engineering integrity has improved, the proportion of accidents resulting human error has increased. In over 75% of cases the actions of the crew have been identified as a major contributory factor [2] making human error the primary risk to flight safety.

Human Factors in aviation is intimately associated with the pursuit of safety. It is embedded in selection, training and design processes and is a cornerstone of all safety management systems. Furthermore, 'good' Human Factors practice is mandated (either implicitly or explicitly) via many airworthiness regulations. This paper examines the treatment of just two of the more pervasive aspects of Human Factors encountered throughout the airworthiness regulations: error and workload.

The roots of human error are manifold and have complex inter-relationships with all aspects of the operation of a modern airliner. For example, during the last decade, as a result of a series of accidents involving highly automated aircraft (e.g. the accident involving an Airbus A320 at Strasbourg and the Boeing 757 near Cali) 'design induced' error was of particular concern to the airworthiness authorities. The

D. Harris (Ed.): Engin. Psychol. and Cog. Ergonomics, HCII 2011, LNAI 6781, pp. 546–555, 2011.

Federal Aviation Administration (FAA) study of the pilot-aircraft interfaces in highly automated aircraft [3] contained criticisms relating to aspects such as autoflight mode awareness/indication; energy awareness; confusing and unclear display symbology, and a lack of consistency in Flight Management Systems. In 1999 the Department of Transportation tasked the Aviation Rulemaking Advisory Committee to '*review the existing material in FAR/JAR 25 and make recommendations about what regulatory standards and/or advisory material should be updated or developed to consistently address design-related flight crew performance vulnerabilities and prevention (detection, tolerance and recovery) of flight crew error*'. In Europe this has resulted in a new airworthiness rule (CS 25.1302). The US FAA will soon follow in adopting this rule. However, many errors have their root causes in a range of other aspects of the operation of the aircraft, not just flight deck design.

Mental workload assessment has been a component of the flight deck certification process since 1993. Indeed, until the recent implementation of the flight deck certification requirement aimed at avoiding design induced error [4] the assessment of pilot workload was the primary rule associated with Human Factors. Appendix D to FAR/CS 25.1523 and FAA Advisory Circular AC 25-1523-1 define six basic workload *functions* and ten workload *factors* [5]. Workload *functions* are related to the basic tasks of flying the aircraft (e.g. flight path control; navigation; communications): these facets impose workload on the pilots. The workload imposed by these *functions* can be either ameliorated or exacerbated by the workload *factors*. These are aspects that relate to the design of the aircraft and/or its operation, such as the accessibility, ease, and simplicity of operation of all necessary flight, power and equipment controls; the extent of required monitoring of systems, and the degree of automation provided in the aircraft systems to afford automatic crossover to, or isolation of difficulties after failures or malfunctions.

Workload is a stressor that needs controlling. The workload *factors* can all be managed by various aspect of good design. In this context, aircraft certification is concerned with the measurement of the workload imposed by the aircraft and its operation to demonstrate that it is within acceptable bounds for safe fight.

2 Integration and Interdependency

Applegate and Graeber [6] described the increasing levels of integration and interdependency of aircraft systems in Boeing jet transport aircraft. Early airliners such as the Boeing 707 and 727 had relatively independent systems managed by a Flight Engineer. The initial Boeing 737s had simplified systems with greater levels of automation for the management of systems to allow two crew operations. Nevertheless, the aircraft still utilized analog technology. Later Boeing 757/767 models were the first to use digital technology. However, their basic architectures were simply digitized versions of earlier analog systems with little integration. The Boeing 777 employed new system architectures with greater use of digital technology. The Boeing 777 possesses highly integrated systems with inputs providing data for a variety of aircraft functions. This increased complexity and integration, though, also impacted upon the system design.

In response to these higher levels of system integration, several industry/ government teams developed corresponding safety requirements and practices (e.g. SAE ARP4754 ‘Certification Considerations for Highly Integrated or Complex Airplane Systems’ [7] and SAE ARP4761 ‘Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems’ [8]). However, the airworthiness regulations themselves, as contained in Code of Federal Regulations, Title 14 (Aeronautics and Space); Part 25 (Airworthiness standards: Transport Category Airplanes) still continue to adopt a ‘system-by-system approach’. Aircraft systems (or perhaps more properly now, ‘functions’) are still considered largely on an engineering, standalone basis with little consideration for their integration.

In addition to aircraft becoming more integrated, airline operations have also become more integrated. Consider the turn-round operation which has traditionally been viewed as a standalone process with responsibilities shared between the airline and airport. Emphasis in operations is now becoming placed upon synchronizing all stakeholders. ATM (Air Traffic Management) links the arrival, turn-round and departure phases as one entity. The associated ground processes and en-route traffic are now considered as part of a time-dependent chain. Airport Collaborative Decision Making (CDM) is used as a mechanism to integrate airports into the ATM network. The CDM turn-round process includes airport operator, airline, air traffic control, ground handling and Central Flow Management Unit. Flight update messages and departure planning information are in place to inform all participating CDM partners about a particular flight’s progress [9]. In addition, the nature of the airline business has changed dramatically. There is now a great deal more outsourcing and sub-contracting of functions previously undertaken within an airline. Organizationally, airlines are now semi-‘open’ systems (in terms of Systems Theory [10]). To illustrate, airlines operate into a wide range of airports; maintenance is often provided by third parties and ATM/ATC is provided by the national authorities of the countries which they either operate into or overfly. Furthermore, some low-cost airlines may not even own their aircraft, employ their own ground and check-in personnel, and in extreme cases, may not even employ their own pilots [11].

However, as a result of airlines simultaneously becoming more organizationally ‘open’ while also exhibiting a much higher degree of integration of operations, it has become easier for errors to promulgate between organizations [12]. For example, the error proximal to the accident in the Uberlingen mid-air collision was a failure of the Skyguide air traffic controller in Zurich Air Traffic Control Centre to notice that two aircraft were on converging flight paths. This error was then compounded and promulgated across organizations when the controller also gave incorrect positional information concerning the conflicting Boeing 757 to the crew of the Tupolev Tu-154M when they expedited their descent: he also failed to notice that the Boeing had initiated a descent in response to a TCAS advisory. These errors were partially a result of his workload being high because he was the only controller on duty and he was overloaded because he was simultaneously trying to coordinate the approach of an Airbus A320 into the nearby Friedrichshafen airport.

3 Regulatory Framework

In many respects, the airworthiness regulations addressing Human Factors issues are extremely fragmented. For the sake of this discussion the US regulatory structures will be used to illustrate, as covered in Part 25 of the Code of Federal Regulations (CFR), Title 14 (Aeronautics and Space) [13].

Over the last 50 years, so as to accommodate all the different facets of airline operations, the commercial aviation system has developed a rule system has become increasingly diverse and complex. For example, the basics of pilot licensing and training are covered Part 61 of the Federal Aviation Regulations (FARs). These are supplemented by further license endorsements to fly an aircraft at night, fly an aircraft with more than one engine, fly in controlled airspace, etc. To fly fare-paying passengers requires an Airline Transport Pilots certificate. The regulations covering training technology (e.g. flight simulators) are covered in Part 60 of the regulations. The basic rules for the operation of aircraft are covered in FAR Part 91. FAR Part 119 applies to the operation of a civil aircraft as an air carrier or commercial operator. This specifies the management roles and processes required for an Air Operator's Certificate (largely organizational issues). The manner in which an airline's operations are conducted is specified in Part 121, 125 and/or 135 (further organizational and operational matters).

From a Human Factors perspective, Part 25 deals with the flight deck interfaces, which are covered in a number of separate regulations; as noted earlier licensing, training and the technology of training are covered Parts 61 and 60. These training-associated parts of the regulations are all generic requirements but once an aircraft weighs over 12,500 lbs a specific type rating is required which ensures that there is a good 'fit' between the aircraft, and the pilot's skills, knowledge and ability to fly it (a product of training). Organizational structures and function are dealt with in Parts 119, 121, 125 and 135. This can be further illustrated by superimposing the various parts of the regulations over a simple representation of a classical 'Perception-Decision-Action-Feedback' loop which describes a simple manual flying task (see Figure 1). The aircraft controls and displays are part of the aircraft and hence are regulated in Part 25. The basic skills required to fly an aircraft and their assessment is covered in Part 61: the flight simulator technology to inculcate these skills is considered in Part 60. However, how the pilot uses these components in an airline context (i.e. how the task of flying an aircraft containing passengers and cargo is undertaken) and the 'fit' between the aircraft and pilot is regulated in Parts 121/125/135. Flying the airplane in a safe and appropriate manner within the air traffic system is covered in Parts 91 and 119 and the wider environmental context of operations (not considered in Figure 1) includes yet more parts of the regulations, such as Part 71 (Designation of Class A, B, C, D, and E Airspace Areas; Air Traffic Service Routes; and Reporting Points); Part 77 (Objects Affecting Navigable Airspace); Part 139 (Certification of Airports) and Part 153 (Airport Operations). This brief description merely begins to scratch the surface of the complexity and fragmentation of the regulations. However, the one thing that the rules are not explicitly concerned with is the *system* of transporting people and cargo safely from A to B, despite this being their intent.

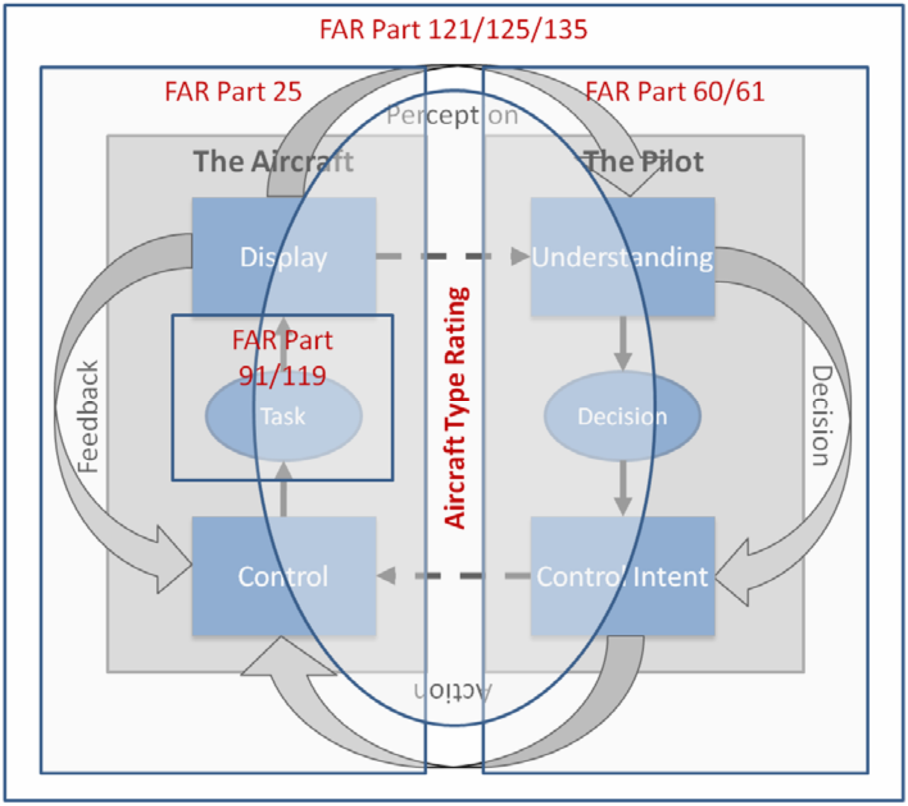

Fig. 1. The concept of the Human-Machine (Flight Deck) Interface superimposed over a representation of the classical 'Perception-Decision-Action-Feedback' control loop with the various parts of FARs further superimposed over the diagram to illustrate the fragmentation of the regulatory system (adapted from Harris [14])

4 Systemic Nature of Workload and Error

Pilot workload is a product of the number and difficulty of the tasks to be performed in the time available; the usability of the flight deck equipment and the interactions with the flight task and other stressors. The topic of pilot workload appears in 37 different FAA Advisory Circulars relating to 19 separate parts of the regulations. The system objective should be to manage pilot's workload but this is handled in different ways across the various parts of the rules. Most often, the regulatory requirement is simply that the component/function under consideration should not impose unduly high levels of workload; but how can this be achieved without the wider consideration of other aspects, such as the procedures involved; design of the flightdeck equipment; the other tasks being performed simultaneously and the environmental context?

Error in the operation of large commercial aircraft appears in 45 FAA Advisory Circulars across 24 parts of the regulations all addressing different parts of the socio-technical system of operating an airliner. However, the systemic view of error is that it is a product of equipment design, procedures, training and the environment [15]. It has also been described how errors can promulgate across organizational boundaries. Error has its roots in the surrounding socio-technical system. Again, the system objective is to manage error but there is no regulatory systemic approach to the eradication, control and management of error (the classical error 'troika').

When the consideration of these issues is described in this manner it becomes apparent that the regulatory structures impede making system-wide improvements in safety and efficiency. If workload and error have a system-wide etiology, they must be regulated collectively across the many separate aspects of the system of regulation if they are to be tackled efficiently and effectively. It may be the case that it is the regulatory system itself that is preventing further improvements in safety (hence the observation that during the last decade the serious accident rate has plateaued at approximately one per million departures). Simply adding another local regulation to fix one specific aspect of a much wider system problem is unlikely to have any major effect. Fragmented rules that do not adopt a system-wide perspective may not increase safety to the degree anticipated.

Many Human Factors issues lie not within an individual regulation but between regulations. The new European Human Factors flight deck certification rule (CS 25.1302[5]) tries to take a task-based approach but is limited by the scope of Part 25 itself (which addresses only the design of the aircraft). Factors outside Part 25 cannot be considered when assessing compliance, nor is it permitted that the regulation can address issues outside those associated with the design and structure of the aircraft. While the probability of design-induced error on the flight deck may be significantly reduced after implementation of this rule, the level of overall risk in flight operations and the accident rate may only be marginally decreased as a result of this failure to adopt a systemic perspective: not all errors on the flight deck fall into the category of 'design induced'. In fact, to suggest that there is merely a single source to any error is over-simplistic. To re-iterate, error and workload are products of interactions between the pilots, aircraft, procedures and the environment. The notion of human error having a single root cause is an oversimplified view of the roots of failure. Furthermore, flying an aircraft progresses on a task-by-task basis *not* a system-by-system basis (the approach implicit in the structure of the regulations). The regulatory structures are not commensurate with human performance.

Consider the following case study of the Singapore Airlines Flight 006 accident, in Taipei, Taiwan. Workload and error were both involved in the sequence of events but the source and/or control of these factors cannot be isolated within any one single part of the regulations. Furthermore, error can result from factors external to the aircraft (but which are still covered within the wider regulatory structures).

4.1 Singapore Airlines Flight 006, Boeing 747, Taipei, Taiwan, 2000

Flight SQ006 crashed on departure from Taipei airport at night in heavy rain and strong winds from a passing typhoon. The accident was attributed to a lack of situational awareness which resulted in the crew erroneously taking off from the wrong runway.

The crew was in a hurry to depart before the weather deteriorated further, closing the airport. They were cleared for departure on runway 05L as runway 05R was closed between taxiways N4 and N5 owing to construction work; as a result, runway 05R was re-designated as taxiway NC. The wind was reported as 36 knots (gusting to 56 knots) with a runway visual range of 600 meters. Upon reaching the end of the taxiway the crew turned right into taxiway N1 and immediately made a 180-degree turn onto runway 05R. After very short hold SQ006 started its takeoff roll. Just after V1 (the go/no-go decision speed) the aircraft hit concrete barriers, excavators and other construction equipment, crashing back onto the runway and then breaking up and bursting into flames [16]. Seventy-nine passengers (out of 159 on board) and four of the 20 crew died.

The reasons contributing to the decision to takeoff from the wrong runway were attributed to a variety of causes, including: poor CRM (the crew did not ensure they understood the correct route to runway 05L and no one confirmed which runway they had entered); there was misleading runway/taxiway lighting leading onto runway 05R resulting in the Captain focusing his attention on following these taxiway centre-line lights; crew workload was much higher than normal as a consequence of the inbound typhoon; and the environmental conditions were poor (strong crosswind, low visibility and slippery runway). There was information available on the flightdeck suggesting that the aircraft was on the incorrect runway (e.g. the runway edge lighting not illuminated; there were lighting configuration and width differences between Runway 05L and 05R; and the para-visual display indicated that the aircraft was not aligned with the runway localizer) but these factors were ignored.

In this example aspects of CRM; pilot training; airport design and operation; environment (weather factors imposing workload); Air Traffic Control and flightdeck display design were all implicated in the sequence of events leading to the accident. If examined using the FAA regulatory structures, Parts 60 (Flight Simulation Training Device Initial and Continuing Qualification and Use) and 61 (Certification: Pilots, Flight Instructors, and Ground Instructors) were implicated in the training of the pilots. The oversight of aircraft operations would be subject to overview under Part 135 (Operating requirements: Commuter and on demand operations and rules governing persons on board such aircraft). The regulation of the airport itself would be covered under Parts 139 (Certification of Airports) and 153 (Airport Operations). The design of the aircraft flightdeck and its equipment is covered under Part 25 (Airworthiness standards: Transport Category Airplanes). However, the errors made and the workload imposed on the crew cannot be attributed to any one single factor (hence any one part of the regulations). To re-iterate, the causes of workload and error are systemic.

5 A Safety-Case Approach

The current aviation safety-related regulatory structure has evolved over five decades, or more. It began when engineering considerations took precedence and when aircraft systems were relatively independent. As the reliability and structural integrity of aircraft has improved, human error has become the primary risk to flight safety. However, in recent years the serious accident rate has remained relatively constant at approximately one per million departures. It has been suggested that this plateau in the accident rate may be at least partially attributable to the fragmentary nature of the regulations when dealing with Human Factors. The structure of the aviation-safety regulations is not compatible with human behavior which progresses on a task-by-task basis not on a system-by-system basis.

Furthermore, aviation accidents rarely have a single error or cause underlying them:

> *'…it is well established that accidents cannot be attributed to a single cause, or in most instances, even a single individual. In fact, even the identification of a "primary" cause is fraught with problems. Instead, aviation accidents are the result of a number of causes...'* (Shappell and Wiegmann, p. 60 [17]).

The regulations were also developed at a time when airline operations were much simpler, lower tempo and were less integrated. During this period airlines were also more organizationally -'closed'. However, safe working practices are dependent upon the control management exercises over work processes and factors external to the organization.

Fragmented rules that do not afford a system-wide perspective may not increase safety to the degree anticipated. From a Human Factors perspective a coherent link between aircraft design, training and operations is required to enhance both safety and efficiency that is also commensurate with human behavior. Rules and regulations need to be future proof, defined in terms of the required result not the method to achieve it. Airworthiness rules that are too prescriptive may stifle technological and operational innovation and also potential advances in safety.

Generation of an operational Safety Case may be a regulatory approach which satisfies the requirements of these criteria and is compatible with the nature of both human behavior and modern airline operations. Safety Cases are commonly used in the UK offshore oil and gas industry. Each installation must demonstrate (to the UK Health and Safety Executive) how major accident hazards are adequately controlled and that the management system is suitable. This approach to Safety Management was mandated after the accident to the Piper Alpha oil production platform in the North Sea in 1988 that killed 167 personnel [18]. At this time the offshore multinational companies operated the installations largely with their own personnel. However, during the last twenty years oil companies have restructured and in common with the airline industry, sub-contracting has become commonplace.

The Safety Case is a structured argument, supported by a body of evidence that provides a comprehensive and valid case that a system is safe for a particular type of operation in a particular operating environment. From a Human Factors perspective specific topics under consideration in safety case presentations normally cover the competencies required to perform the work; training and training needs analysis; development and maintenance of procedures; communication processes; manning levels; automation and allocation of function; supervision of staff; shift patterns; hardware and software layout; environmental performance shaping factors; human error potential and safety culture. Safety Cases are not prescriptive: the aim is to demonstrate systems meet the required safety goal; they do not separate the human from the system; they are evidence-based and are subject to continual revision (they change in response to changes in the nature of operations). This approach is also becoming used much more frequently in defense aerospace, for example in the Eurofighter Aircraft Avionics project; the BAe Hawk Aircraft Safety Justification and in Military Air Traffic Management Systems. A similar approach is being use for the safety evaluation of civil Unmanned Air Systems [19]. Furthermore, the basis for safety cases is already being used by all airlines as part of their Safety Management Processes.

If safety regulation is to progress in a manner compatible with the management of workload and error it has to progress on a systemic basis, not a system-by-system basis. A Safety Case-based approach provides this opportunity. This is not to say that it should replace the current set of regulations as this would be completely impractical. However, it can be used as an adjunct and/or alternative where a suitable waiver to existing regulations is granted.

References

1. Boeing Commercial Airplane Group: Statistical Summary of Commercial Jet Airplane Accidents Worldwide Operations 1959–2008. Boeing Commercial Airplane, Seattle, WA (2009)
2. Civil Aviation Authority: Global Fatal Accident Review 1997–2006 (CAP 776). Civil Aviation Authority, London (2008)
3. Federal Aviation Administration. Report on the Interfaces between Flightcrews and Modern Flight Deck Systems. US Department of Transportation, Washington, DC (1996)
4. Federal Aviation Administration: Advisory Circular AC 25-1523-1 Minimum Flight Crew. US Department of Transportation, Washington, DC (1993)
5. European Aviation Safety Agency: Certification Specifications for Large Aeroplanes (CS- 25): Amendment 7. EASA, Cologne, `http://www.easa.europa.eu/ws_prod/g/rg_certspecs.php#CS-25`
6. Applegate, J.D., Graeber, R.C.: Integrated safety systems design and human factors considerations for jet transport aeroplanes. Human Factors and Aerospace Safety 1, 201–221 (2001)
7. Society of Automotive Engineers: Certification Considerations for Highly Integrated or Complex Airplane Systems (SAE ARP4754). Society of Automotive Engineers, Warrendale, PA (1996)
8. Society of Automotive Engineers: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems (SAE ARP4761). Society of Automotive Engineers, Warrendale, PA (1996)
9. Groppe, M., Pagliari, R., Harris, D.: Monitoring the Aircraft Turn-Round Process: Applying a Qualitative Cognitive Model Based on Field Observations. In: Droog, A., Heese, M (eds) Performance, Safety and Well-being in Aviation: Proceedings of the 29th Conference of the European Association for Aviation Psychology, Budapest, Hungary, September 20-24, pp. 266-277. European Association for Aviation Psychology, Amsterdam, NL (2010)
10. von Berthalanfry, L.: General systems theory: general systems. Yearbook of the Society of General Systems Theory, 1, 1-10 (1956)
11. Harris, D.: Keynote Address: An Open Systems Approach to Safety Culture: Actions, Influences and Concerns. In: Australian Aviation Psychology Association (AAvPA) International Conference – Evolving System Safety, Sydney, Australia, November 9–11. Australian Aviation Psychology Association, Victoria (2006)

12. Harris, D., Li, W.-C.: An Extension of the Human Factors Analysis and Classification System (HFACS) for use in Open Systems. Theoretical Issues in Ergonomics Science (in press)
13. Code of Federal Regulations Title 14: Aeronautics and Space. Part 25: Airworthiness standards: Transport Category Airplanes. National Archives and Records Administration, Washington DC, `http://www.gpo.gov/nara/cfr`
14. Harris, D.: Human Factors for Flight Deck Certification: Issues in Compliance with the new European Aviation Safety Agency Certification Specification 25.1302. Journal of Aeronautics, Astronautics and Aviation. Series A 42, 11–20 (2010)
15. Dekker, S.W.A.: The Re-Invention of Human Error. Human Factors and Aerospace Safety 1, 247–266 (2001)
16. Aviation Safety Council: Aircraft Accident Report: Crashed on a Partially Closed Runway During Takeoff. Singapore Airlines Flight 006 (Boeing 747-400, 9V-SPK); CKS Airport, Taoyuan, Taiwan, October 31, 2000. ASC, Taiwan, Republic of China (2002)
17. Shappell, S.A., Wiegmann, D.A.: Applying Reason: the Human Factors Analysis and Classification System (HFACS). Human Factors and Aerospace Safety 1, 59–86 (2001)
18. Cullen, The Honourable Lord: The Public Inquiry into the Piper Alpha Disaster. HM Stationery Office, London (1990)
19. Civil Aviation Authority: Unmanned Aircraft System Operations in UK Airspace – Guidance (CAP 722). Civil Aviation Authority, London (2010)