Evaluating human error data for hazards in air-traffic control and deriving a quantitative safety index

Takeshi Matsuoka* and Osamu Amai

Air Traffic Management Department,
Electronic Navigation Research Institute,
National Institute of Maritime, Port and Aviation Technology,
7-42-23, Jindaijihigashi-machi, Chofu, Tokyo, 182-0012, Japan
Email: mats@mpat.go.jp
Email: mats@cc.utsunomiya-u.ac.jp
Email: amai@mpat.go.jp
*Corresponding author

Abstract: We developed an analysis method of hazards related to air-traffic control (ATC). We used mixing approach procedures such as required navigation performance, authorisation required (RNP AR) and instrument landing system (ILS), as the test case. We carried out the hazard and operability (HAZOP) study and ATC real-time simulation experiments in the situation of the mixed operation for finding the hazards because we were not able to find them as the result of literature examination. We collected the data required for this analysis in the simulation experiment and selected HAZOP as the key assessment methodology. The hazard analysis method developed enables to perform a quantitative HAZOP analysis. We quantified the likelihood of accidents and the ratios between the hazard severities at the development stage. Furthermore, we discussed a safety index based on the statistics of recent catastrophic air accidents around the world. A safety index matrix showed the regions of acceptable levels with mitigation by a quantitative index value.

Keywords: air-traffic control; ATC; RNP AR; instrument landing system; ILS; human error rate; risk matrix; safety level; quantitative risk index; HAZOP analysis.

Reference to this paper should be made as follows: Matsuoka, T. and Amai, O. (2019) 'Evaluating human error data for hazards in air-traffic control and deriving a quantitative safety index', *Int. J. Aviation Management*, Vol. 4, No. 3, pp.199–223.

Biographical notes: Takeshi Matsuoka received his BSc and MSc degrees in Physics from Tokyo Institute of Technology in 1968 and the University of Tokyo in 1972, respectively. He joined the Ship Research Institute in 1977. From 1979 to 1980, he studied at the Massachusetts Institute of Technology. Then, he has been engaging in the probabilistic safety assessment (PSA), system reliability analysis. He received his Doctor of Engineering from the University of Tokyo in 1987. He developed a new system reliability analysis methodology GO-FLOW, which can easily analyse large, complex systems. He also developed a method for reliability analysis of logical loop structure by using algebraic solution of Boolean equation. He became a Professor of Utsunomiya University in 2006. Currently, he is a Lecturer of Utsunomiya University, and a Visiting Researcher of Air Traffic Management division, Electronic Navigation Research Institute.

Osamu Amai received his BE and ME degrees in Electric Engineering from the Science University of Tokyo in 1986 and 1988, respectively. He joined the Electronic Navigation Research Institute (ENRI) in 1988. He has been engaged in extensive studies related to air traffic control systems. In particular, he has studied safety assessment methodology for aircraft separation minima. He received his Doctor of Engineering from the Tokyo University of Marine Science and Technology in 2015. He is currently working as a Principal Researcher in Air Traffic Management division. He is now interested in hazard assessment methodology and real-time simulation technique.

1 Introduction

Recently, many airports have adopted the required navigation performance, authorisation required (RNP AR) approach procedures (ICAO, 2009); they are used at over 100 airports in the US and at approximately 30 airports in Japan. However, for a given runway, RNP AR is currently not combined with other approach procedures, e.g., instrument landing system (ILS). Devlin et al. (2005) studied operating RNP AR and ILS simultaneously (hereinafter referred to as mixed RNP AR/ILS) for parallel runways, and Thipphavong et al. (2012) simulated the mixed operation at a Phoenix Sky Harbor International airport in the US. For airports without parallel runways, studies on the feasibility of safe mixed operations among several approach procedures for the same runway are emerging (Amai et al., 2014; Fujita and Amai, 2013).

We performed the present study by the following steps. We begin developing air-traffic control (ATC) procedures for mixed RNP AR/ILS using goal-structuring notation (GSN) diagrams. Then, identification of hazards in mixed RNP AR/ILS was performed by the hazard and operability (HAZOP) analysis. We collected and evaluated human error (HE) data and background factors related to ATC for the HAZOP analysis. Severity of accidents and occurrence frequencies are quantified based on the statistical data and other information. We proposed the quantified risk matrix, safety criteria and quantitative HAZOP analysis. Lastly, we have performed preliminary quantitative HAZOP analysis.

2 Safety assessment of mixed RNP AR/ILS

Various methods have been proposed to identify and evaluate hazards. Herein, we base our safety assessment on the HAZOP method (British Standards, 2002). HAZOP is a structured and systematic method for examining a complex process or operation with the aim of identifying and evaluating problems that may represent risks to personnel or equipment.

The RNP AR approach procedures enable the curved approach by using radius to fix leg (RF-leg) in the vicinity of the runway. Straight flight path length is only necessary about one nautical mile in that situation. On the other hand, ILS approach procedures need straight flight path length at least five nautical miles. In the case of all aircraft which fly under ILS approach procedures, that is called ILS aircraft, air-traffic controllers ensure the safety by maintaining longitudinal separation by physically aligning. In the case of mixed operation of the ILS aircraft and the aircraft, which fly under RNP AR approach procedures and approach by using the curved approach in the vicinity of the runway, controllers however cannot physically align these aircraft. And the controller needs not one-dimensional thinking but two-dimensional thinking. This probably makes new hazards. It is very interesting for us. To investigate them, we developed ATC procedures for mixed RNP AR/ILS by constructing GSN diagrams. We then transformed the ATC procedures into a flow chart to understand them easily and clearly. We performed the HAZOP analysis based on this flow chart as well as identified hazards and evaluated risks in mixed RNP AR/ILS. We also identified hazards by analysing the behaviour of air-traffic controllers in simulator experiments with mixed RNP AR/ILS (Amai and Matsuoka, 2015). The simulation experiments are the human-in-the-loop simulations. These employed a subject who plays the role of terminal radar controller by former real controller and persons who play the role of pilots.

A safety case is a structured argument supported by evidence and can be used to justify the decision to accept a certain system as being safe. Various fields have now adopted the safety case approach. In the realm of ATC, the European Organization for the Safety of Air Navigation (EUROCONTROL) has been studying how to apply the safety case approach to ATC systems (EUROCONTROL, 2006).

Figure 1 An example of GSN diagram (see online version for colours)

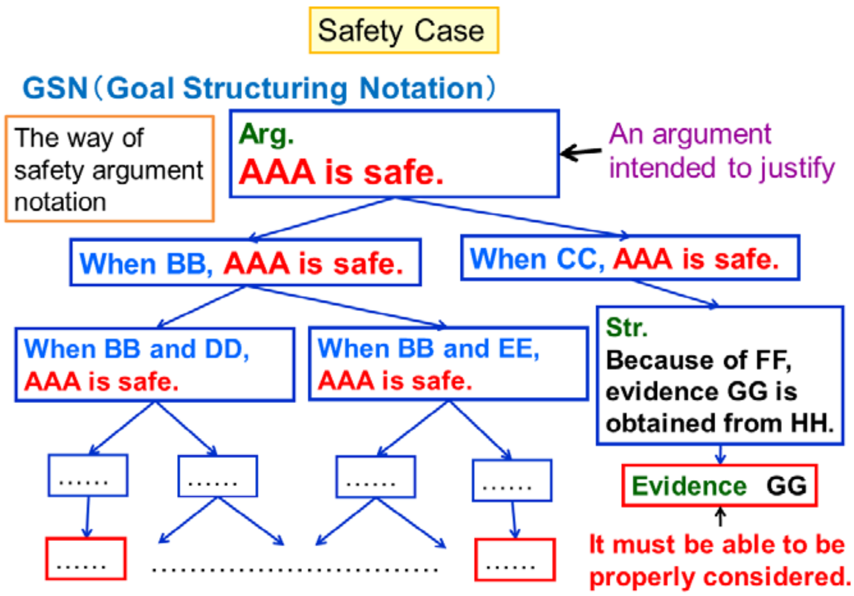

Figure 1 shows an example of the GSN diagrams developed in this analysis. In the figure, ‘Arg.’ means argument and ‘Str.’ means the strategy used to test the argument.

3 HE rates

3.1 Human reliability analysis

In ATC procedures, many tasks rely on human endeavours, but perfect human performance cannot be guaranteed. Therefore, it is necessary to develop a method for evaluating human reliability. The procedure for assessing HEs, known as human reliability analysis (HRA), is divided into three steps. In the first step, a series of human activities is decomposed into elementary actions that can be evaluated as human factors. Such actions can be found in HE data handbooks and analysis textbooks. In the second step, performance-shaping factors (PSFs) that influence the HEs associated with each elementary action identified in the first step are identified. The final step is to estimate the HE probabilities (HEPs) for the elementary actions. There are many methods for quantifying HEPs, such as deduction from field data, Bayesian estimation, expert judgement, and simulation. The probabilities of occurrence of errors range from 10^{-5} to 1.0 in general and from 10^{-3} to 10^{-2} for well-trained activities (Kirwan, 1964).

The first formulated HRA method was the technique for HE rate prediction (THERP) due to Swain et al. (1963). The use of THERP to the reactor safety study (Rasmussen report) (USNRC, 1975; Swain and Guttman, 1983) was epoch making for probabilistic safety assessment (PSA). Since then, many sophisticated and usable HRA methods have been developed, all of which are based on THERP. They are classified into three generations. First-generation methods do not consider human cognition when performing PSA. An example of first-generation HRA is the SPAR-H (standardised plant analysis risk HRA) method (Gertman et al., 2005) developed by the US Nuclear Regulatory Commission (USNRC) and Idaho National Laboratory. Second-generation HRA methods [e.g., ATHEANA ('a technique for human event analysis') (USNRC, 2000) and the cognitive reliability and error analysis method (CREAM) (Hollnagel, 1998)] do consider cognition and for situations of error occurrence (Context). Third-generation methods (the most recent ones) observe human actions in computer generated actual scenarios and environmental conditions, often making a model of decision-making processes and human's dynamic actions. An example of third-generation methods is the Micro Saint simulation software (Schunk et al., 2003).

In the present study, we collected HEP data, PSFs, and related information, which we arranged for easy use in air-traffic management (ATM) safety analysis (HAZOP-based analysis), especially for mixed RNP AR/ILS. In Table 1, we list the identified HEPs, which are mainly in the realm of ATM activities; we divide the human activities into 13 main categories. For each HEP value, we cite the relevant reference(s) in the final column for confirmation.

Table 1 List of HEPs

Item	*Description*	*HEP*	*Reference*
Human activity (general)	Highest obtainable reliability (minimal error rates)	$\mathbf{10^{-4}}$ (one person) 10^{-5} (group)	Kirwan (1964)
Simple routine	Simple, familiar, and frequent tasks; skill-based or rule-based	$\mathbf{4 \times 10^{-4}}$ $(1.4 \times 10^{-4} – 9 \times 10^{-4})$	Hickling (2007) Gertman et al. (2005)
	Omission	$\mathbf{1 \times 10^{-3}}$ 3×10^{-3}	Swain and Guttman (1983) USNRC (1975)
	Selection error	$\mathbf{3 \times 10^{-3}}$	Swain and Guttman (1983)
	Forgetting	$\mathbf{3 \times 10^{-3}}$	Swain and Guttman (1983)
	Delay of judgment	$\mathbf{3.8 \times 10^{-3}}$	Liu and Li (2014)*[1]
Nontrivial familiar	Familiar, relatively frequent task, requiring knowledge-based performance and judgment.	$\mathbf{1.6 \times 10^{-2}}$	Hickling (2007)
	Normal tasks involving deviation from planned operations	$(1.2 \times 10^{-2} – 2.8 \times 10^{-2})$	Thommesen Andersen (2012)
Communication, routine	Familiar content routinely conveyed, and where at least a limited template for communication is available	$\mathbf{6 \times 10^{-3}}$	Kirwan and Gibson (2007)
	Highly proceduralised	$\mathbf{2 \times 10^{-3}}$	Thommesen and Andersen (2012)
Communication, non-routine	Unforeseen, novel content, with no template	$\mathbf{3 \times 10^{-2}}$	Kirwan (1964)
Emergency scenarios – known	Tasks characterised by some urgency and stress due to safety or production concerns, for which a plan of action (a template/a script) and relevant information are available	$\mathbf{1 \times 10^{-1}}$	Kirwan (1964)
Emergency scenarios-unknown	Uncertain information, without procedure	$\mathbf{3 \times 10^{-1}}$	Kirwan (1964)

Notes: Values in boldface are those selected for the present study.
Values in parentheses are lower and upper limit values.
*1: time-out probability in simulator experiment
*2: ‘fail to notice major cross-roads’.
*3: misreading the information in simulator experiment.
*4: misunderstanding the procedure text in simulator experiment.
*5: commission error probability in nuclear plants.
*6: test or inspection error probability in nuclear plants
*7: omission error probability in monitor display in nuclear plant control room.

Table 1 List of HEPs (continued)

Item	*Description*	*HEP*	*Reference*
Cognition errors	Misunderstanding	$\mathbf{5 \times 10^{-4}}$	Smith (2005)*[2]
	Reading error of information	$\mathbf{4.5 \times 10^{-3}}$	Liu and Li (2014)*[3]
Misinterpretations	Misinterpretations with correct recognition	$\mathbf{2 \times 10^{-2}}$ $(4.2 \times 10^{-3} - 1 \times 10^{-1})$	Gertman et al. (1992)
	Misinterpretations	$\mathbf{7.8 \times 10^{-4}}$	Liu and Li (2014)*[4]
Diagnosis errors	Diagnosis error	$\mathbf{2.14 \times 10^{-2}}$	USNRC (1994)*[5]
	Diagnosis error without situation awareness	$\mathbf{1 \times 10^{-2}}$	Swain and Guttman (1983) and Gertman et al. (2005)
	At initial diagnosis	$\mathbf{2 \times 10^{-1}}$	USNRC (1994))
Judgment errors	With large workload	$\mathbf{9.2 \times 10^{-2}}$ $(2.9 \times 10^{-2} - 2.9 \times 10^{-1})$	Gertman et al. (1992)
	Misjudgment	4.1×10^{-3} $\mathbf{2.5 \times 10^{-3}}$	USNRC (1994)*[6] Liu and Li (2014)
Preoccupation, distraction, and diverted attention	Error in one activity among multiple tasks	$\mathbf{1.2 \times 10^{-2}}$ $(1.2 \times 10^{-1} - 1.2 \times 10^{-3})$	Gertman et al. (1992)
	Resulted in omission	$\mathbf{1.8 \times 10^{-2}}$	USNRC (1994)*[7]
Violation	Intentional violation of procedures and violation of rules	$\mathbf{8.7 \times 10^{-3}}$ $(1.6 \times 10^{-3} - 4.7 \times 10^{-2})$	USNRC (1994)
Dare to act	Awareness and task execution related to hazards/damage	$\mathbf{1.6 \times 10^{-2}}$	Haney (2002)

Notes: Values in boldface are those selected for the present study.
Values in parentheses are lower and upper limit values.
*1: time-out probability in simulator experiment
*2: 'fail to notice major cross-roads'.
*3: misreading the information in simulator experiment.
*4: misunderstanding the procedure text in simulator experiment.
*5: commission error probability in nuclear plants.
*6: test or inspection error probability in nuclear plants
*7: omission error probability in monitor display in nuclear plant control room.

3.2 HEs in ATC activities

In THERP, error probabilities and PSFs were specified for various human actions and tasks. After THERP, USNRC assembled data on hardware failures and HEs for risk analysis. The HEP data were collected from all the nuclear reactors in the US and several outside the US, and a comprehensive database was made in the form of the nuclear computerised library for assessing reactor reliability (NUCLARR) (USNRC, 1994). In the field of aviation, the US Federal Aviation Administration (FAA) has developed the human factors analysis and classification system (HFACS) (FAA, 2000), which is widely used for accident analyses but does not provide HEP data. Meanwhile, Europe has the computerised operator reliability and error database (CORE-DATA) (Gibson and Megaw, 1999), which is used by the likes of the UK Health and Safety Executive (UKHSE) and EUROCONTROL as well as for research (e.g., Kirwan, 2006). However, CORE-DATA is not open to the public, and we cannot access the raw data. Thommesen and Andersen (2012) estimated HEPs and PSFs based on CORE-DATA and gave precise data.

In the realm of ATC, Kirwan and Gibson (2007) has listed the causes of HEs. In the Netherlands, the National Aerospace Laboratory has made a hazard model for ATM and also a comprehensive list of the causes of hazards (National Aerospace Laboratory, 2011). The ATM is a dynamic, integrated management of air-traffic and airspace, including ATC, airspace management (ASM) and air-traffic flow management (ATFM). We distinguish ATC and ATM by contents properly. EUROCONTROL has developed a detailed methodology for analysing HEs in ATM, including all forms of error and their causal, contributory, and compounding factors. The resultant approach for analysing HEs is called the 'HE in ATM technique' (HERA-JANUS) (Isaac et al., 2003).

3.3 Performance-shaping factors

The quality of human performance depends on the conditions under which the tasks or activities are carried out. These conditions are generally referred to as PSFs. If human actions are required under abnormal conditions or in an emergency situation, the HEPs associated with the actions will increase. In Table 1, each HEP is that under normal conditions and is referred to as the nominal HEP (HEP_N). In THERP (first-generation HRA), the effects of PSFs were assumed to be obtained as certain quantitative values, and they were listed. An HEP under a specific condition is obtained from the associated HEP_N by multiplying the latter by the associated PSF value listed in Table 2. This method is used in the present analysis because it is simple and allows various conditions to be considered. Table 2 lists the PSFs collected in the present study, which are mainly under ATC conditions. Also, the associated references are cited in the final column for confirmation.

Table 2 Values of PSFs

Condition	*Value of PSFs*	*Reference*
Without alarms	50	Swain and Guttman (1983)
Ergonomic design (inadequate)	2–10	Swain and Guttman (1983)
Human–machine interface (HMI) ambiguous	2–10 4 2	Swain and Guttman (1983) Gertman et al. (2005) Gertman et al. (1992)
HMI feedback (inadequate)	5.5	Williams (1988)
Delayed feedback and imperfect feedback	4	Thommesen and Andersen (2012) and RSSB (2004)
No labels	10	Swain and Guttman (1983)
Lack of supervision/checks	2	Swain and Guttman (1983) and Gertman et al. (1992)
Lack of moral or safety culture	2	RSSB (2004) and Gertman et al. (1992)
Without motivation	4	Gertman et al. (1992)
Without procedures	4 3 2	Gertman et al. (2005) Swain and Guttman (1983) Gertman et al. (1992)
Lack of rules and manuals	3	Swain and Guttman (1983)
Insufficient information and knowledge	3	RSSB (2004)
Without training/experience	3	Gertman et al. (1992, 2005)
Without refresher training	2	Swain and Guttman (1983)
Sufficient training/experience	0.5	Gertman et al. (2005)
Support by different methods or procedures	0.1	Thommesen and Andersen (2012)
Lack of communication	3	Gertman et al. (1992)
Lack of tense atmosphere	2	Swain and Guttman (1983) and Gertman et al. (2005)
Urgent correspondence/extreme stress	5	Thommesen and Andersen (2012) and Gertman et al. (2005)
High stress	2	Gertman et al. (2005) and Swain and Guttman (1983)
Heavy tasks, step by step	2	Swain and Guttman (1983)
Heavy tasks, dynamic	5	Swain and Guttman (1983)
Extremely high stress, step by step	5	Swain and Guttman (1983)
Multiple tasks at the same time	6	Thommesen and Andersen (2012)
Extremely high stress, dynamic	0.25 (HE prob.)	Swain and Guttman (1983)
Extremely complex tasks	5	Gertman et al. (2005)
Complex tasks	2	Thommesen and Andersen (2012) and Gertman et al. (2005)

Notes: 'HE prob.' means the value of HEP.

Table 2 Values of PSFs (continued)

Condition	*Value of PSFs*	*Reference*
New tasks	3–5	Thommesen and Andersen (2012)
Conflict between the required tasks	3	RSSB (2004)
Overwork	5 4	Swain and Guttman (1983) Gertman et al. (1992)
Available time duration equals required time duration	10	Swain and Guttman (1983) and Gertman et al. (2005)
Available time duration is 5 times the required time duration	0.1	Gertman et al. (2005)
Available time duration is 50 times the required time duration	0.01	Swain and Guttman (1983) and Gertman et al. (2005)
Time pressure		
1 min	1.0 (HE prob.)	Swain and Guttman (1983)
5 min	0.9 (HE prob.)	Swain and Guttman (1983)
10 min	0.6 (HE prob.)	Swain and Guttman (1983)
30 min	0.1 (HE prob.)	Swain and Guttman (1983)
120 min	0.01 (HE prob.)	Swain and Guttman (1983)

Notes: 'HE prob.' means the value of HEP.

If multiple conditions affect a task, we must consider multiple PSFs simultaneously. We calculate HEPs with multiple PSFs as follows based on the method embodied in SPAR-H (Gertman et al., 2005). First, we calculate a composite PSF score (PSF_C) by simply multiplying the PSFs. We then calculate the resultant HEP as follows from HEP_N and PSF_C:

$$\text{HEP} = \frac{(HEP_N \times PSF_C)}{\left(HEP_N \times (PSF_C - 1) + 1\right)} \tag{1}$$

For example, consider the 'diagnosis error without situation awareness: $HEP_N = 0.01$' (second value of tenth category in Table 1) with the PSFs of 'ergonomic design (inadequate): PSF = 10', 'without refresher training: PSF = 2', and 'complex task: PSF = 2)' in Table 2. In this case, PSF_C is 10 × 2 × 2 = 40 and the resultant HEP is

$$\text{HEP}=\frac{0.01 \times 40}{\left(0.01 \times (40-1)+1\right)} = 0 \cdot \frac{4}{1} \cdot 39 = 0.29 \tag{2}$$

3.4 Causes of HEs

Kirwan and Gibson (2007) performed controller-action reliability assessment (CARA), in which error-producing conditions are considered specific to the ATC context. Such conditions are predicted to negatively influence controller performance, thereby increasing the HEPs associated with controller tasks. As error-producing conditions, 22 fundamental items are listed in Table 3. The list provides important information about hazard identification, risk assessment, and effective actions to increase safety.

Table 3 Error-producing conditions

No.	*EPC description*
1	A need to unlearn a technique and apply one which requires the application of an opposing philosophy
2	Unfamiliarity, i.e., a potentially important situation that only occurs infrequently or is novel
3	Time pressure
4	Traffic complexity leading to cognitive loading
5	Difficulties caused by poor position handover or shift handover practices
6	Difficulties caused by team coordination problems, friction between team members, or inter-centre difficulties
7	Controller workplace noise/lighting issues, cockpit smoke
8	Weather
9	On-the-job training
10	Cognitive overload, particularly one caused by simultaneous presentation of non-redundant information
11	Poor, ambiguous or ill-matched system feedback
12	Shortfalls in the quality of information conveyed by procedures
13	Low vigilance or fatigue
14	Controller shift from anticipatory to reactive mode
15	Risk taking
16	High emotional stress and effects of ill health
17	Low workforce morale or adverse organisational environment
18	Communications quality
19	Over or under-trust in system or automation
20	Unavailable equipment/degraded mode
21	Little or no independent checking (e.g., lack of two pairs of eyes when needed)
22	Unreliable instrumentation or tool

Source: Kirwan and Gibson (2007)

3.5 Background factors for HEs in ATC activities

The National Aerospace Laboratory in the Netherlands conducted the MAREA project (Mathematical Approach towards Resilience Engineering in ATM) (National Aerospace Laboratory, 2011). That project listed 525 very precise and definite hazards related to aircraft systems, pilots, ATC systems, speech-based communication, controller activities, and others. In the present study, we add to that list the items adopted in HFACS (FAA, 2000) and HERA-JANUS (Isaac et al., 2003), categorised and rearranged. We then make a large list of the items 'action error', 'kind of error', and 'background or condition for errors'. We use the list to make the HAZOP worksheet for assessing the safety of mixed RNP AR/ILS. Table 4 gives part of that list as an example.

Table 4 Errors and backgrounds (examples)

Action error	*Kind of error*	*Background or condition*
• Identification of a non-existent conflict • Controller makes a reading error • Controller does not detect a deviation from a clearance • The controller fails to separate two aircraft before transfer • Controller interprets information or traffic situation wrongly • Controller makes wrong decision, while interpretation of information is correct • Controller provides wrong message. while decision is correct • The controller instructed a greater speed control than was necessary • The controller requested the correct aircraft to the wrong direction • The controller requested the wrong aircraft to the wrong direction • The controller requested the correct descent to the wrong aircraft • Controller ignores an alert (no evaluation) • Controller wrongly evaluates traffic situation after an alert • Controller is distracted by an alert • Controller corrects the wrong aircraft • Controller is not aware of the failure of malfunctioning of a technical system	• Risk of a conflict is underestimated • Controller spends too much time on monitoring • Over-reliance on system data • Inaccurate automated references • Smaller spacing leads to more time pressure • Alert causes attention tunnelling • Controller is confused about position as communicated by pilot	• Change of ATC procedures leads to more errors in controller's performance • Controller is overloaded with information • Automation makes controller's tasks more complex • Controller receives contradictory information • Charts/notices are contradictory • Alert interrupts task scheduling of controller • Increase in communication load • Loss of monitoring skills (due to automation) • Complacency of controller • Large workload of controller • Difficulty in tracking aircraft/vehicles

4 Severity of accidents and incidents

The FAA has released the *FAA Safety Management System Manual Ver. 4* (FAA, 2014), in which severity and likelihood are defined as follows. Severity is categorised 'catastrophic', 'hazardous', 'major', 'minor', or 'minimal'. Examples of definite events are listed for ATC services, unmanned aircraft systems, aircraft passengers, and national airspace system (NAS) equipment and flight crew. Table 5 lists the hazard conditions for ATC services and aircraft passengers.

Table 5 Hazard conditions for ATC services and flying public

Minimal	*Minor*	*Major*	*Hazardous*	*Catastrophic*
A minimal reduction in ATC services, CAT D runway, incursion, proximity event, operational deviation, or measure of compliance greater than or equal to 66%	Low risk analysis event severity, two or fewer indicators fail CAT C Runway Incursion	Medium risk analysis event severity, three indicators fail CAT B Runway Incursion	High risk analysis event severity, four indicators fail CAT A Runway Incursion	Ground collision Mid-air collision Controlled flight into terrain or obstacles
Minimal injury or discomfort to persons on board	Physical discomfort to passenger(s) (e.g., extreme braking action, clear air turbulence causing unexpected movement of aircraft resulting in injuries to one or two passengers out of their seats) Minor injury to less than or equal to 10% of persons on board	Physical distress to passengers (e.g., abrupt evasive action, severe turbulence causing unexpected aircraft movements) Minor injury to greater than 10% of persons on board	Serious injury to persons on board	Fatal injuries to persons on board

Source: FAA (2014), Table 3.4: Hazard Severity Definitions

Likewise, likelihood is categorised as 'frequent', 'probable', 'remote', 'extremely remote', or 'extremely improbable', and the expected occurrence rates are as given in Table 6. The values in Table 6 were derived from an analysis of historical ATC data mapped to the established engineering standards (FAA, 2002) and can be applied to both ATC and flight procedures. The range of each expected occurrence rate was determined through calculations made using ten years of aviation data.

Table 6 Likelihood; quantitative value

	Operations: expected occurrence rate (per operation/flight hour/operational hour)*
	Quantitative (ATC/flight procedures/systems engineering)
Frequent	$P \geq 1$ per 10^3
Probable	1 per $10^3 > P \geq 1$ per 10^5
Remote	1 per $10^5 > P \geq 1$ per 10^7
Extremely Remote	1 per $10^7 > P \geq 1$ per 10^9
Extremely Improbable	1 per $10^9 > P \geq 1$ per 10^{14}

Notes: *It is important to note that the close correlation between flight hours and operations is entirely coincidental; average flight time is roughly two hours, and each flight has about two tower and two TRACON operations. The two numbers are not interchangeable.

Source: FAA (2014), Table 3.6: Likelihood of the effect standards

Table 7 Cost to society per case proposed by UKHSE

Severity	*Cost*	*Rate*
1 person's death	1,575,000 pounds	1
Severe injury	27,700 pounds	0.018
Slight injury	880 pounds	0.00056

Source: UKHSE (2017), Table 2: Cost to Britain per case

For the quantitative HAZOP analysis, we must estimate the ratios of hazard severities because no such ratios are given in the *FAA Safety Management System Manual* (FAA, 2014). Therefore, we based the ratios on discussions in other fields. The UKHSE has proposed the quantitative relations given in Table 7 among deaths and injuries arising from occupational accidents (UKHSE, 2017), where the costs are those for occupational accidents. Thus, we calculated the quantitative ratios among the injury severities as listed in the third column. In Table 7, 'severe injury' means that the injured worker is absent for seven days or more, and 'slight injury' means absence of up to six days.

One person's death or injury cannot correspond directly to the severity of the accident as defined by the FAA. A catastrophic air-traffic accident is one in which an aircraft crashes and more than 100 people (occasionally as many as 500 people) die, thereby generating a huge economic loss. The price of a new model of a large aircraft is 400–500 million pounds (Airbus Press Centre, 2016; AircraftCompare.com, 2016), equivalent to the deaths of 250–300 people. A catastrophic accident also causes loss of quality of life, insurance payments, and investigation. All these are categorised as common costs and are estimated to be nearly 38% (except property cost) of the fatality cost (Commonwealth of Australia, Bureau of Transport Economics, 1999). Aircraft incidents are also likely to incur costs due to delays and disruption, and such costs are expected to be substantial (Commonwealth of Australia, Bureau of Transport Economics, 1999). Considering all these effects, the severity of 'catastrophic' is estimated to be nearly 1,000 times larger than that of one person's death in an occupational accident.

The second category of severity of an air-traffic accident is ‘hazardous’, in which several people (five to ten people or a certain percent of the number of people on board) are seriously injured. The severity of ‘hazardous’ is almost equivalent to that of one person’s death in an occupational accident.

The third category of severity of an air-traffic accident is ‘major’, in which more than 10% of the people on board suffer minor injuries; this equals to more than 10–50 people suffering minor injuries. There is no category of air-traffic accident that relates directly to ‘severe injury’ as defined for an occupational accident. If all 50 people are slightly injured, the corresponding severity ratio becomes 0.028 (= 0.00056 [slight injury in occupational accident] × 50). Because some people will be injured more seriously, the actual multiplier will be around 65. Thus, the severity of the ‘major’ category is considered to be 0.036.

The fourth category is ‘minor’, in which one or two passengers out of their seats are injured or at most 10% of the people on board suffer minor injuries. This corresponds to one or two people being slightly injured in an occupational accident, making the multiplier around 2. Thus, the severity of the ‘minor’ category is considered to be 0.00112. There is no fourth category in an occupational accident. The ratio 32 (= 0.036/0.00112) falls between ‘major’ and ‘minor’ air-traffic accidents. Therefore, the severity of the ‘minimal’ category is also considered to be 32 times smaller than that of ‘minor’.

Table 8 Calculation of the ratios between severities of hazard conditions

Occupational accident		*Multiplier*	*Air traffic accident*		
Severity	*Ratio*		*Hazard condition*	*Comparison to occupational accident*	*Ratio*
1 person’s death	1	×1,000	Catastrophic	1,000	1
		×1	Hazardous	1	1×10^{-3}
Slight injury	0.00056	×65	Major	0.036	3.6×10^{-5}
		×2	Minor	0.00112	1.1×10^{-6}
		Minor × 1/32	Minimal	0.000035	3.5×10^{-8}

The above discussions are summarised in Table 8. In the final column, the ratios among the severities of the hazard conditions are those obtained for air-traffic accidents.

5 Risk matrix and safety criteria

5.1 Risk matrices proposed by FAA and ICAO

The combination of ‘severity’ and ‘likelihood’ creates the risk level. The FAA has proposed a safety risk matrix (FAA, 2006) based on this combination, and safety criteria are defined as shown in Figure 2. This figure is conceptual, and no numerical values are given. Safety levels are categorised as ‘acceptable’, ‘acceptable with mitigation’, and ‘unacceptable’. The ICAO also uses a matrix to discuss safety levels and gives a similar risk matrix to that shown in Figure 3 (ICAO, 2013). In Figure 3, red, yellow, and green characters correspond to the safety levels ‘unacceptable’, ‘acceptable with mitigation’, and ‘acceptable’, respectively.

Figure 2 Safety risk matrix proposed by FAA, conceptual idea (see online version for colours)

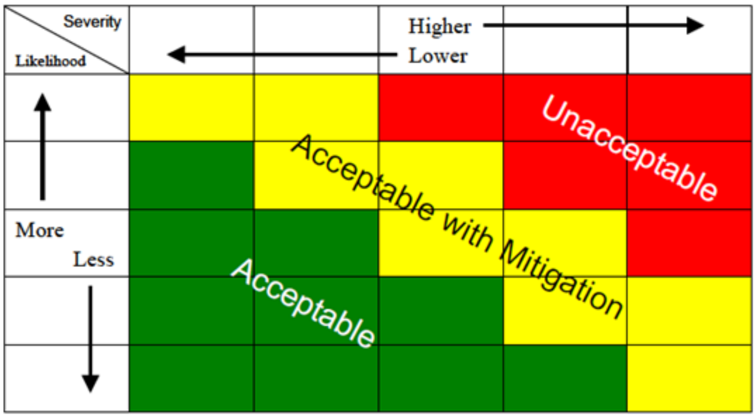

Figure 3 Safety risk assessment matrix proposed by ICAO (see online version for colours)

Risk probability		Risk severity				
		Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E

5.2 *Quantification of risk matrix*

Likelihood values are assigned in the *FAA Safety Management System Manual Ver. 4* (FAA, 2014), as given in Table 6. The severity ratio was discussed in section IV, and the values are given in the final column of Table 8. With these numerical values, risk levels can be expressed by as a numerical index, for example the product of likelihood and severity ratio. In that case, the unit of the index becomes per operational hour or per flight hour ('/fh').

Safety levels are classified according to the ICAO proposal as shown in Figure 4. The upper limit of likelihood is given for each category in Figure 4, so the largest index value is written at each position. The upper limit of 'acceptable with mitigation' lies in the range 1×10^{-8}/fh to 1.1×10^{-6}/fh depending on the severity level. We reason that an index value of 1.1×10^{-6}/fh is unacceptable for any severity condition based on the ICAO classification. The values for 'acceptable risk' lie in the range 3.6×10^{-14}/fh to

1×10^{-12}/fh depending on the severity level. We also reason that an index value of 3.6×10^{-14}/fh is acceptable for any severity condition, that is, without any particular condition.

Figure 4 Safety risk matrix with numerical values (see online version for colours)

			Risk Probability				
			Extremery Improbable	Extremery Remote	Remote	Probable	Frequent
			1.00E-09	1.00E-07	1.00E-05	1.00E-03	1
Risk Severity	Catastrophic	1	1.00E-09	1.00E-07	1.00E-05	1.00E-03	1
	Hazadous	0.001	1.00E-12	1.00E-10	1.00E-08	1.00E-06	1.00E-03
	Major	0.00003	3.60E-14	3.60E-12	3.60E-10	3.60E-08	3.60E-05
	Minor	0.000001	1.10E-15	1.10E-13	1.10E-11	1.10E-09	1.10E-06
	Minimal	0.000000035	3.50E-17	3.50E-15	3.50E-13	3.50E-11	3.50E-08

Figure 5 Modified safety risk matrix with numerical values (see online version for colours)

			Risk Probability				
			Extremery Improbable	Extremery Remote	Remote	Probable	Frequent
			1.00E-09	1.00E-07	1.00E-05	1.00E-03	1
Risk Severity	Catastrophic	1	1.00E-09	1.00E-07	1.00E-05	1.00E-03	1
	Hazadous	0.001	1.00E-12	1.00E-10	1.00E-08	1.00E-06	1.00E-03
	Major	0.00003	3.60E-14	3.60E-12	3.60E-10	3.60E-08	3.60E-05
	Minor	0.000001	1.10E-15	1.10E-13	1.10E-11	1.10E-09	1.10E-06
	Minimal	0.000000035	3.50E-17	3.50E-15	3.50E-13	3.50E-11	3.50E-08
		Acceptable:	1.50E-12			Unacceptable:	1.09E-07

5.3 *Quantification of safety criteria*

We examined the safety levels for current worldwide aviation by using eight years of recent aviation records. From 2008 to 2015, there were 15 catastrophic accidents killed more than 100 people per one accident. The total number of flying hours of commercial jet aircraft per year is 5×10^7 fh (Boeing, 2015), making the occurrence frequency of catastrophic accidents 3.75×10^{-8}/fh (= 15 cases/8 y/5 $\times$ 10^7 fh). During descent, approach, and landing, the rate of fatal accidents is nearly 2.9 times that in all flight stages (Boeing, 2015). The occurrence frequency of catastrophic accidents around the airport area is 1.09×10^{-7}/fh. Now, considering catastrophic accidents, for which the severity ratio is 1.0, the index of safety level (product of likelihood and severity ratio) becomes 1.09×10^{-7}/fh. This value is considered to be the upper limit of the 'acceptable with mitigation' level. This value is also considered to be the lower limit of the 'unacceptable' level. That is, the value of 1.09×10^{-7}/fh marks the boundary between 'acceptable with mitigation' and 'unacceptable'.

As examples of acceptable risk, the US Environment Protection Agency (USEPA) has proposed a cancer risk of 10^{-6}/life (USEPA, 2000), and the USNRC has proposed that an increase of 0.1% in civilian life risk for cancer and accidents is acceptable (USNRC, 1983). The corresponding value is around 5×10^{-6}/life. Also, the UKHSE has proposed 1×10^{-6}/y as an acceptable level of occupational risk, which is equivalent to 1.4×10^{-6}/life for the risk of civilian life (UKHSE, 2001). Therefore, the value of 1×10^{-6}/life is an acceptable level in civilian life and is equivalent to 1.5×10^{-12}/h. The occurrence of catastrophic accidents with less than 1.5×10^{-12}/fh is apparently acceptable without any particular condition.

We re-evaluate the safety risk matrix in Figure 5 with the above two values, namely 1.09×10^{-7}/fh (upper limit of the 'acceptable with mitigation' level) and 1.5×10^{-12}/fh (upper limit of the 'acceptable without any particular condition'). The index values in the matrix are the upper limits at the corresponding positions. For example, the index value for the catastrophic/remote combination is 1.0×10^{-5}/fh, which actually means that index values between 1.0×10^{-7}/fh and 1.0×10^{-5}/fh are included at this position. Therefore, the levels 'unacceptable' and 'acceptable with mitigation' are included at this position, as indicated by the pink colour. The combinations of hazardous/probable, major/frequent, and minor/frequent are in the same situation and are also indicated by pink. For similar reasons, the positions coloured light green include the 'acceptable' risk level.

These index values may change according to social perceptions of safety levels, which depend on technological innovations, peoples' attitudes, and so on. In that case, we should change the numerical values in the safety risk matrix accordingly.

6 HAZOP worksheet

HAZOP was used originally to analyse chemical plants. For the present analysis, we developed a modified HAZOP worksheet with which to analyse ATC generally and mixed RNP AR/ILS in particular. Tables 9a to 9c show the HAZOP worksheet developed for the present study. Selected items are in this worksheet. For each ATC procedure, first identify 'deviation or abnormal state from a normal condition', in the seventh column from the left in Table 9a. Then the reason or cause of this deviation is described from the fourth to the sixth column in Table 9a and effects to the subsystem or total system for each item are written in the left-side columns in Table 9b. If all the items are evaluated and the risk level is determined adequately, a specific ATC procedure has been assessed. After all the procedures have been assessed, the total risk level of the ATC system is evaluated and the safety or otherwise of this ATC system (e.g., mixed RNP AR/ILS) is determined. In the present study, we present a new method; quantitative HAZOP analysis which is possible by using quantitative safety criteria.

Table 9a HAZOP worksheet – (left part) (see online version for colours)

Starting point in this HAZOP

ID	*Component*	*Function/operating mechanism of a component*	*Cause of failure, back ground factor for HE, environmental condition*	*Event type*	*HE/failure mode*	*Deviation or abnormal state from a normal condition*
2			4. traffic complexity leading to cognitive loading 13. low vigilance or fatigue 16. High emotional stress and effects of ill health	Omission	Preoccupation distraction diverted attention	While watching the distance between two ILS aircraft, controller fails overlooks an RNR AR aircraft coming flying from another direction
3			2. Unfamiliarity, i.e., a potentially important situation which only occurs infrequently or is novel	Misjudgement	Judgement error	Estimation error for arrival time of RNP AR aircraft

Table 9b HAZOP worksheet – (middle part)

Effects of deviation		*Method to detect error or unsafe situation*	*Method of recovering or restoration*	*Severity of effect (qualitative expression)*	*Severity of effect (quantities)*	*Precondition of occurrence of deviation (occurrence rate or occurrence number)*	*Description of precondition*
To surrounding system or components	*To total system or air traffic control*						
There will be near-miss between ILS and AR, just before runway. Increase of workloads by additional operation.	Dissolution of near-miss causes the confusion of total air traffic	Pilot confirms to ATC. Double watch. Automatic alarm system		Minor	7.2E-07	6.3E-01	There may be 5 times among 50 trials based on the simulation.
There will be near-miss between ILS and AR. Increase of workloads by unusual separation distance.	Dissolution of near-miss causes the confusion of total air traffic. Delay of departure flight.	Pilot confirms to ATC.		Minor	7.2E-07	9.0E-01	Maximum number of RNP AR aircraft

Table 9c HAZOP worksheet – (right part)

PSF (performance shaping factor)	*Value of PSF*	*Occurrence probability of deviation under the precondition*	*Risk*	*Risk after reduction (mixed operation)*	*Risk after reduction (general)*	*Risk level*	*Comments*
Task complexity	2	1.2E-02	1.1E-08	1.5E-12		Acceptable with mitigation	If AR aircraft follows separate traffic, there is small hazard.
Task complexity	2	2.5E-03	3.2E-09	1.5E-12		Acceptable with mitigation	Landing order can be changed. There is no problem.

In the preliminary analysis, we identified and evaluated 59 items (ATC procedures), two of which had index values that were less than acceptable risk level. Those two items were 'instruction to ILS aircraft for holding to prioritise RNP AR aircraft' and 'instruction to ILS aircraft for diversion to prioritise RNP AR aircraft'. The index values of the other items were evaluated less than unacceptable level. Proper mitigation would lead to higher safety levels. The preliminary analysis has shown no problems with mixed RNP AR/ILS regarding safety.

7 Summary of contents

We have studied the feasibility of safety assessment methods for safe mixed operation among several approach procedures on a given runway at an airport without parallel runways. For this purpose, we collected basic data, investigated analysis methods, and presented a quantitative index. As basic data on ATM activities, we collected HEPs, PSFs, error-producing conditions, and background factors of HEs. Regarding the analysis method, we selected HAZOP as the key methodology for assessing safety. We used a safety case approach for the preliminary analysis and identified hazards using a flowchart of ATC procedures and by simulator experiments (Amai and Matsuoka, 2015). The FAA has categorised the severity of hazards and likelihood of accidents and assigned values for likelihood, and the UKHSE has given the costs to society of occupational accidents. Based on these quantitative values, we determined the ratios among hazard severities in an ATM system.

The safety risk matrices presented by the FAA and ICAO give acceptable risk levels conceptually but lack quantitative values. Instead, we used the product of expected occurrence probability and ratio of hazard severities (i.e., likelihood × severity ratio) as a safety index. With this index, safety levels can be quantified in a safety risk matrix.

We discussed the upper limit of the 'acceptable with mitigation' level based on recent statistical data on catastrophic air accidents around the world; we estimated the level as 1.07×10^{-7}/fh. The USEPA has proposed a risk of 10^{-6}/life as acceptable without any conditions, so we used that value as the acceptable risk level in an ATM system, corresponding to 1.5×10^{-12}/fh. We modified the safety risk matrix using those two values and gave quantitative acceptable risk levels. We presented a new method; quantitative HAZOP analysis which is possible by using quantitative safety criteria, that is, a safety index and two values of safety levels.

8 Conclusions

We are now performing a feasibility analysis of safe mixed operation among several approach procedures on a given runway at an airport without parallel runways. We selected HAZOP as the key methodology of the feasibility analysis. For the HAZOP analysis, we quantified the likelihood of accidents and the ratios among hazard severities. We discussed a safety index based on recent statistical data on catastrophic accidents around the world. The quantified safety risk matrix showed the areas of the 'acceptable with mitigation' and 'unacceptable' levels according to the quantitative index values and we understood the areas are valid in comparison to the risk matrices of ICAO and FAA. We presented a new method, quantitative HAZOP analysis, and the preliminary analysis showed no problem with mixed RNP AR/ILS regarding safety. Following that preparatory work, we are now engaged in assessing the safety of mixed RNP AR/ILS with the support of the Ministry of Land, Infrastructure, Transport and Tourism of the Japanese government.

References

Airbus Press Centre (2016) [online] http://www.airbus.com/presscentre (accessed 24 August 2016).

AircraftCompare.com (2016) [online] http://www.aircraftcompare.com/ (accessed 24 August 2016).

Amai, O. and Matsuoka, T. (2015) 'Air traffic control real-time simulation experiment regarding the mixed operation between RNP AR and ILS approach procedures', *Proceedings of the 2015 International Association of Institutes of Navigation World Congress*, Prague, Czech Republic, 20–23 October.

Amai, O., Fujita, M. and Matsuoka, T.(2014) 'On a safety analysis of the mixed operation of RNP AR (required navigation performance-authorization required) approach procedure and conventional approach procedures by developing safety case documents', *SSS(Safety), The Institute of Electronics, Information and Communication Engineers*, Vol. 114, No. 4, pp.9–12, (in Japanese).

Boeing (2015) *Statistical Summary of Commercial Jet Aircraft Accidents Worldwide Operations | 1959–2014* [online] https://www.skybrary.aero/bookshelf/books/3198.pdf (accessed 10 July 2018).

British Standards (2002) *Hazard and Operability Studies (HAZOP studies) –Application Guide*, BS. IEC61882:2002.

Commonwealth of Australia, Bureau of Transport Economics (1999) *Cost of Civil Aviation Accidents and Incidents*, Report-98 [online] https://bitre.gov.au/publications/1998/files/report_098.pdf (accessed 10 July 2018).

Devlin, C., Mills, M., Ottobre, R., Porter, S. and Sprong, K. (2005) 'Applications and benefits of RNP approaches in the United States National Airspace System', *AIAA 5th ATIO and 16th Lighter-Than-Air Sys Tech. and Balloon Systems Conferences*, Arlington.

EUROCONTROL (2006) *Safety case Development Manual*, EUROCONTROL DAP/SSH/091.

Fujita, M. and Amai, O. (2013) 'Initial study of mixed approach procedure and its safety analysis method', *SSS(Safety) The Institute of Electronics, Information and Communication Engineers*, Vol. 113, Nos. 54, pp.1–4 (in Japanese).

Gertman, D., Blackman, H., Marble, J., Byers, J. and Smith, C. (2005) *The SPAR-H human Reliability Analysis Method*, NUREG/CR-6883 [online] https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6883/cr6883.pdf.

Gertman, D.I., Blackman, H.S., Haney, L.N., Seidler, K.S. and Hahn, H.A.(1992) 'INTENT: a method for estimating human error probabilities for decision based errors', *Reliability Engineering and System Safety*, Vol. 35, No. 2, pp.127–136.

Gibson, W.H. and Megaw, T.D. (1999) *The Implementation of CORE-DATA, A Computerized Human Error Probability Database*, HSE Contracted Research Report 245/1999.

Haney, L.N. (2002) *Framework for Assessing Notorious Contributing Influences for Error (FRANCIE): Overview and Generic User Guidance*, INL/EXT-01-01014, Idaho National Laboratory [online] https://inldigitallibrary.inl.gov/sites/sti/sti/2761702.pdf.

Health and Safety Executive (UKHSE) (2001) *Reducing Risks, Protecting People HSE's Decision-Making Process*, *HSE Books*, ISBN 0 7176 2151 0.

Health and Safety Executive (UKHSE) (2017) *Costs to Britain of Workplace Fatalities and Self-Reported Injuries and Ill Health, 2013/14* [online] http://www.hse.gov.uk/statistics/pdf/cost-to-britain.pdf (accessed 10 July 2018).

Hickling, N. (2007) *An Independent Review of a Rail-Specific Human Reliability Assessment Technique for Driving Tasks*, Report T270, Rail Safety and Standard Board, UK.

Hollnagel, E. (1998) *Cognitive Reliability and Error Analysis Method (CREAM)*, Elsevier, Oxford.

International Civil Aviation Organization (ICAO) (2009) *Required Navigation Performance Authorization Required (RNP AR) Procedure Design Manual*, ICAO Doc 9905, 1st ed.

International Civil Aviation Organization (ICAO) (2013) *Safety Management Manual (2013), Chapter 5 Safety Management System (SMS)*, Doc 9859.

Isaac, A., Shorrock, S. T., Kennedy, R., Kirwan, B., Andersen, H. and Bove, T. (2003) *The Human Error in ATM Technique (HERA-JANUS)*, EUROCONTROL HRS/HSP-002-REP-03 [online] https://www.eurocontrol.int/sites/default/files/field_tabs/content/documents/nm/safety/the-human-error-in-atm-technique.pdf.

Kirwan, B. (2006) *Feasibility Study into the Collection of Human Error Probability Data*, EEC Note No. 02/06 [online] https://www.eurocontrol.int/sites/default/files/library/005_Human_Error_Probability_Data%20.pdf.

Kirwan, B. and Gibson, H. (2007) 'CARA: a human reliability assessment tool for air traffic safety management – technical basis and preliminary architecture', *The Safety of Systems, Proceedings of the Fifteenth Safety-critical Systems Symposium*, Bristol, UK, 13–15 February, pp.197–214.

Kirwan, B.A. (1964) *Guide to Practical Human Reliability Assessment*, Taylor and Francis, London.

Liu, P. and Li, Z. (2014) 'Human error data collection and comparison with predictions by SPAR-H', *Risk Analysis*, Vol.34, No. 9, pp.1706–1719.

National Aerospace Laboratory (2011) *Hazards in ATM: Model Constructs, Coverage and Human Responses*, E.02.10-MAREA-D1 [online] http://complexworld.eu/wiki/images/c/cf/E.02.10-MAREA-D2.1-v1.15_(Final).pdf.

Rail Safety and Standard Board (RSSB) (2004) *Rail-Specific Human Reliability Assessment Technique for Driving Tasks*, Final report, Report of Rail Safety and Standard Board, UK [online] http://www.rssb.co.uk/pdf/reports/research/T270_rb_final.pdf.

Schunk, D.W., Bloechle, W.K. and Laughery, R. (2003) 'Micro saint sharp simulation software', *Proceedings of the 2003 Winter Simulation Conference*, New Orleans, Louisiana, USA.

Smith, D.J. (2005) *Reliability, Maintainability and Risk*, 7th ed., Elsevier.

Swain, A. D. and Guttman, H. E. (1983) *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, Final report, NUREG/CR-1278 [online] https://www.nrc.gov/docs/ML0712/ML071210299.pdf.

Swain, A.D., Altman, J.W. and Rook Jr., L.W. (1963) 'Human error quantification', *A Symposium. SCR-610*, Sandia Corporation, Albuquerque.

Thipphavong, J., Jung, J., Swenson, H., Martin, L., Lin, M. and Nguyen, J. (2012) 'Evaluation of the terminal sequencing and spacing system for performance-based navigation arrivals', *31st Digital Avionics System Conference*, 14–18 October, Williamsburg, Virginia, USA.

Thommesen, J. and Andersen, H. B. (2012) *Human Error Probabilities (HEPs) for Generic Tasks and Performance Shaping Factors (PSFs) Selected for Railway Operations*, DTU Report 3.

US Environmental Protection Agency (USEPA) (2000) *Methodology for Deriving Ambient Water Quality Criteria for the Protection of Human Health*, Report of the US Environmental Protection Agency, EPA 822-B-00-004 [online] https://www.nj.gov/drbc/library/documents/EPA_human-health-criteria2000.pdf.

US Federal Aviation Administration (FAA) (2000) *The Human Factors Analysis and Classification System – HFACS*, DOT/FAA/AM-00/7 [online] https://www.nifc.gov/fireInfo/fireInfo_documents/humanfactors_classAnly.pdf.

US Federal Aviation Administration (FAA) (2002) *Advisory Circular 25.1309-1B, System Design and Analysis* [online] https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25.1309-1A.pdf.

US Federal Aviation Administration (FAA) (2006) *Advisory Circular 120-92* [online] https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_120-92B.pdf.

US Federal Aviation Administration (FAA) (2014) *The FAA Safety Management System Manual Ver.4* [online] http://vsgc.odu.edu/ACRPDesignCompetition/2015/Resources%20for%20Design%20Competion%20Website/FAA%20Safety%20Management%20System%20Manual.pdf.

US Nuclear Regulatory Commission (USNRC) (1975) *Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, WASH-1400, NUREG-75/014 [online] https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr75-014/.

US Nuclear Regulatory Commission (USNRC) (1983) *Safety Goals for Nuclear Power Plant Operation*, NUREG-0880 Revision 1 [online] https://www.nrc.gov/docs/ML0717/ML071770230.pdf.

US Nuclear Regulatory Commission (USNRC) (1994) *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) Part 2: Human Error Probability (HEP) Data*, NUREG/CR-4639 EGG-2458, Vol.5, Revision 4 [online] https://www.osti.gov/biblio/10188390.

US Nuclear Regulatory Commission (USNRC) (2000) *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*, NUREG-1624, Revision 1 [online] https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1624/.

Williams, J.C. (1988) 'HEART: a human performance model-based technique utilizing some standard probabilities – a data-based method for assessing and reducing human error to improve operational performance', *IEEE Fourth Conference on Human Factors and Power Plants*, Monterey, CA, USA, 5–9 June 1988, pp.436–450.

List of abbreviations

ASM	airspace management
ATC	air-traffic control
ATFM	air-traffic flow management
ATHEANA	a technique for human event analysis
ATM	air-traffic management
CARA	controller-action reliability assessment
CORE-DATA	computerized operator reliability and error database
CREAM	cognitive reliability and error analysis method
EUROCONTROL	European Organization for the Safety of Air Navigation
FAA	Federal Aviation Administration
GSN	goal-structuring notation diagrams
HAZOP	hazard and operability
HEs	human errors
HEP	human error probability
HFACS	human factors analysis and classification system

HRA	human reliability analysis
HERA-JANUS	HE in ATM Technique
ICAO	International Civil Aviation Organization
ILS	instrument landing system
MAREA	mathematical approach towards resilience engineering in ATM
NAS	national airspace system
NUCLARR	Nuclear Computerized Library for Assessing Reactor Reliability
PSA	probabilistic safety assessment
PSFs	performance-shaping factors
RF-Leg	radius to fix leg
RNP AR	required navigation performance, authorization required
SPAR-H	standardized plant analysis risk HRA
THERP	technique for HE rate prediction
UKHSE	UK Health and Safety Executive
USEPA	US Environmental Protection Agency
USNRC	US Nuclear Regulatory Commission.

List of definitions

HEP_N	nominal HEP
PSF_C	composite PSF score.