Human Factors in Design, Engineering, and Computing, Vol. 238, 2026, 2345–2355
https://doi.org/10.54941/ahfe1008460

System Safety Analysis Considering Human Factors in Aircraft Development

Wu Xu, Ma Shuai, Jia Wanchen, Ding Lin, Miao Chongchong, and Zhang Ruiming

China Aero Polytechnology Establishment, Materiel Human Factors and Ergonomics Laboratory, Beijing 100028, China

ABSTRACT

In conventional system safety analysis approaches, human factors were often overlooked by aircraft designers, as traditional methodologies such Preliminary System Safety Analysis (PSSA) and Functional Hazard Analysis (FHA) primarily focused on system-level failures. With advancements in human factors and ergonomics research, the aviation industry has increasingly recognized the critical role of human elements in safety outcomes. Recent aviation accident statistics indicate that human factors contribute to approximately 70% of incidents, serving as fundamental and complex causal factors. Classic theoretical frameworks such as the Swiss Cheese Model and the REASON model were initially proposed to elucidate the mechanisms of human error occurrence. Subsequent systematic classification systems, including the Skill-Rule-Knowledge model and the Human Factors Analysis and Classification System (HFACS), were developed to standardize human error categorization. Typical pilot performance errors encompass attention allocation failure, cognitive overload, and loss of situation awareness. To quantify the impact of human errors on safety, this study proposes a novel risk assessment methodology integrating human factors into system safety analysis. This approach, termed Human Safety Assessment, enables the identification of potential human error modes and the formulation of mitigation strategies. It is recommended for implementation during the early stages of aircraft development to detect latent human-factor risks and design deficiencies. A human-centered design philosophy is adopted to analyze error propagation through cockpit human-machine interfaces under specific flight scenarios. Furthermore, Human Safety Assessment must be fully integrated with system safety requirements analysis and human factors engineering within the aircraft development lifecycle.

Keywords: Human errors, Systems safety analysis, Human factors, Human safety assessment

INTRODUCTION

System safety remains a critical consideration in engineering disciplines, particularly in the design and operation of complex systems. Traditional safety-assessment methodologies, such as Functional Hazard Assessment (FHA) and Preliminary System Safety Assessment (PSSA), predominantly concentrate on hardware and software failures, thereby neglecting the systemic contribution of human factors to accident sequences. In high-risk

Received August 25, 2026; Revised September 28, 2026; Accepted October 7, 2026; Available online December 1, 2026

© 2026 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

industries including aviation, aerospace, maritime, nuclear, and rail sectors, human errors are now widely acknowledged as a primary driver of catastrophic failures. According to aviation safety reports, the International Civil Aviation Organization (ICAO) attributes approximately 70% of aircraft accidents to human factors, typically characterized by erroneous decision-making, inappropriate attention allocation, and loss of situational awareness. Nevertheless, mainstream safety analysis frameworks persistently lack systematic integration of these human-centric elements during the conceptual design phase. This deficiency may result in systems imposing excessive cognitive demands on operators, thereby inducing novel error modes and ultimately compromising safety integrity.

To address this challenge, a range of human error modeling frameworks have been developed. Reason's Swiss Cheese Model of Accident Causation conceptualizes accidents as the alignment of latent failures across multiple defensive layers, with unsafe human acts serving as critical proximate causes. The Reason's Accident Causation Model further emphasizes the role of organizational and latent conditions in predisposing operators to error-prone behaviors. The Human Factors Analysis and Classification System (HFACS) provides a hierarchical taxonomy for systematically identifying and categorizing human errors across organizational, supervisory, and operational levels. Complementarily, Rasmussen's Skill-Rule-Knowledge (SRK) model offers a theoretical framework for analyzing human cognitive behavior in dynamic, time-pressured environments. While these models elucidate the underlying mechanisms of error generation and provide standardized taxonomies for accident investigation, they are primarily retrospective in nature and often decoupled from the design process, thereby offering limited guidance during the conceptual and preliminary design phases of aircraft and other complex systems.

Amidst the increasing integration of human-centred design principles into engineering practices, recent advancements have facilitated the systematic incorporation of human-factors engineering throughout the system development lifecycle, particularly within safety-critical aviation systems. Furthermore, the proactive identification of potential human-risk vectors during the conceptual design phase not only mitigates the financial burden associated with late-stage design modifications but also substantively improves both safety assurance and operational efficiency.

Despite these advancements, contemporary safety assessment frameworks frequently treat human error as an exogenous variable rather than an intrinsic element of the system design. This conceptual fragmentation creates a persistent disconnect between human factors engineering and system safety engineering, particularly during the conceptual design phases of safety-critical systems like aircraft cockpits. To address this limitation, this study proposes a scenario-model and event-chain based Human Safety Assessment (HSA) methodology that systematically integrates human performance characteristics into the system-safety analysis process. By embedding HSA within established safety-assessment workflows, an operationally robust and quantitatively verifiable

human-risk assessment framework is established, which not only supports aircraft development but also facilitates the implementation of an integrated "human-centred safety" design paradigm.

HUMAN ERROR ANALYSIS BASED ON SCENARIO MODEL

Based on representative mission profiles and operational scenarios, a hierarchical task analysis (HTA) of the human–machine interface is conducted to decompose flight-crew activities into elementary action components. Utilizing the "observe–interpret–plan–execute" taxonomy of cognitive functions, each action component is systematically mapped to its dominant cognitive control mode. Human-error probabilities are quantified through performance-shaping factors derived from the Cognitive Reliability and Error Analysis Method (CREAM), resulting in the development of a predictive human-factors safety index.

CREAM, developed by Hollnagel, represents a second-generation Human Reliability Analysis (HRA) technique explicitly linked to operator reliability within contextual environments. CREAM provides both qualitative and quantitative predictive pathways, with the quantitative mode being implemented only after the completion of qualitative cognitive-task characterization.

Building on this foundation, the present study adopted CREAM's extended quantitative procedure, which refines the fundamental methodology by integrating task-specific cognitive failure events. The analytical protocol is structured into sequential stages:

Task Analysis

Flight procedures extracted from the aircraft operating manual and function list are categorized into mission phases, including "engine start–take-off/climb–cruise–low-level flight–approach/landing–engine shutdown." Each mission phase is further decomposed into sequential operational units. For example, low-level flight is decomposed into "altitude hold–speed hold–destination proximity–decelerate to hover." Each operational unit is then mapped to one of the 15 generic activities defined in CREAM and assigned to one of four cognitive functions (i.e., observe, interpret, plan, and execute).

Common Performance Conditions Assessment

By analyzing the environmental conditions characteristic of flight operations, the impact of each Common Performance Condition (CPC) factor on cognitive task performance is systematically evaluated. Using the human-factor safety of an aircraft cockpit as a case study, the corresponding Performance Shaping Factors (PSFs) are defined. Guided by the cognitive-function failure categories outlined in the CREAM and considering the prevailing levels of PSFs, the dominant human failure event for each cognitive activity within every operational step is identified. This process generates an "aircraft

HMI–operation type–human-error mode" mapping, which is codified in a representative human-failure-mode database. The database is subsequently integrated as a plug-in into the Model-Based Systems Engineering (MBSE) modeling environment, enabling automated instantiation of error modes during the system design phase.

Simultaneously, the acceptability criteria for human-factor safety are established by referencing the aircraft hazard-risk classification scheme. Following the Risk Assessment Code (RAC) procedure outlined in SAE ARP 4761, a human-factor safety risk assessment matrix is constructed (as shown in Table 1), along with the risk acceptance criteria detailed in Table 2.

Table 1: Human-factor safety risk assessment matrix.

Occurrence Probability	Catastrophic	Hazard	Major	Minor
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Extremely Remote	12	15	17	20

Table 2: Human-factor safety risk-acceptance criteria.

Risk Level	Risk Assessment Index	Risk Acceptance Criterion
I	1~5	Unacceptable
II	6~9	Unacceptable – require further decision
III	10~17	Acceptable – subject to review
IV	18~20	Acceptable without review

Predictive Human-Error Probability

The predicted human-error probability (HEP) is calculated through weighted aggregation of the HEP values associated with each cognitive activity identified in the preceding task analysis. The severity of each human error is derived from the functional-failure consequences embedded within the event-chain model, whereas its likelihood is quantified using HRA-based predictive methodologies.

Human Safety Assessment

The aircraft's key operational stakeholders include the captain, first officer, flight engineer, and ground crew. Among these, the aircrews engage with cockpit human–machine interfaces (HMIs) throughout all flight operations. From the pilot's operational perspective, the required control tasks are mapped to identify critical HMI elements, as illustrated in Figure 1, which

includes the following components: flight seats, control devices, instrument panels, and the consoles.



Figure 1: Classification diagram of cockpit human–machine interface types.

Following the clear delineation of the cockpit HMI scope, a scenario-based analysis framework is applied to identify HMIs directly involved in the target task. As a case study, the flight-preparation phase of the take-off scenario is selected to demonstrate the methodology. The operational workflow is systematically decomposed into eight sequential stages: (1) developing the flight plan, (2) completing administrative preparations prior to the take-off checklist, (3) performing the external visual inspection, (4) conducting the interior cockpit inspection, (5) executing pre-start checks, (6) initiating the engine start-up procedure, (7) carrying out engine warm-up and run-up tests, and (8) verifying system status post-start. A systematic human-factors analysis of this sequence identifies potential human-error modes associated with each HMI component, with the synthesized findings consolidated in Table 3.

Table 3: Human error analysis and safety risk assessment.

Activity	Human Errors	Operation Type	Human-Error Mode	Severe Level	Occurrence Probability	Risk Level	Safety Risks
Flight-plan Formulation Initial Engine Start	Loss of flight-plan formulation capability	Touch-screen manipulation	Incorrect value entry Inadvertent touch (false activation)	V	0.003	20	Acceptable without review
Initial Engine Start	Engine fails to start	Switch actuation	Inadvertent touch (false activation) Omission of actuation Reversed control input	V	0.003	20	Acceptable without review
		Lever / stick manipulation	Reversed control input Omission of actuation Excessive control input / over-actuation	V	0.003	20	Acceptable without review

RESULT

The proposed methodology was implemented in a human-factors safety assessment of helicopter operations. Six representative operational scenarios—take-off, flight, landing, loading, sling-load operations, and emergency handling—were systematically modelled to estimate human-error probabilities and identify latent failure modes across the operational and maintenance lifecycle. A total of hundreds of human-factor-related safety risks were quantitatively characterized and prioritized.

Early identification of these risks during the design phase enables engineers to implement mitigation strategies proactively, thereby minimizing cost and schedule overruns associated with late-stage design modifications.

For example, the failure scenario of "loss of single-engine restart capability" under single-engine failure condition was analyzed to identify potential human-error modes and safety risks. In alignment with emergency operation procedures, the pilot's specific operational sequence under single-engine failure conditions was validated through the workflow depicted in Figure 2.

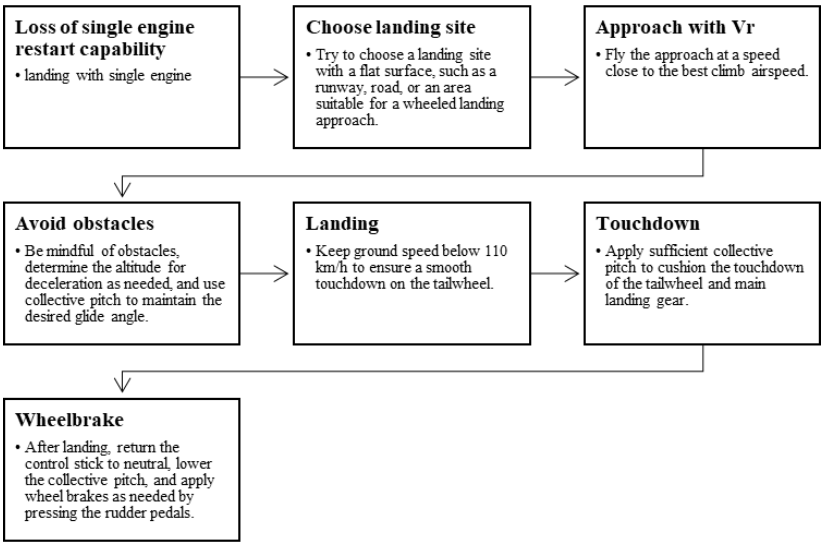


Figure 2: Activity diagram of the flight-preparation scenario.

Under single-engine failure conditions, pilots are required to execute emergency operations based on single-engine landing procedures when the single-engine restart function is lost with an occurrence probability below 1×10^{-5} (safety-critical threshold). Consequently, standardized pilot operation procedures were developed to systematically identify potential human error modes and assess their operational impacts, as detailed in Table 4.

Table 4: Analysis of human errors and impacts.

No.	Procedures	Human Errors	Impact Analysis	Severe Level	Occurrence Probability	Safety Risks
1	Choose landing site	Fail to make the right landing-approach decision	Poor landing-approach selection might increase the difficulty of single-engine landing operations.	C	III	11
2	Approach with Vr	Fail to maintain the right approach speed during landing	Excessive approach speed might increase the difficulty of deceleration during landing.	C	III	11
3	Avoid obstacles	Fail to detect and avoid obstacles	Obstacle avoidance was not performed promptly, resulting in significant time pressure during operation. This might cause damage to the propulsion system and lead to flight accident.	D	II	10

(Continued)

Table 4: Continued.

No.	Procedures	Human Errors	Impact Analysis	Severe Level	Occurrence Probability	Safety Risks
4	Landing	Incorrect decision on deceleration altitude or glide slope maintenance	Misjudgement of deceleration altitude or flight attitude might lead to an excessive glide slope during landing, and result in helicopter ground contact and damage.	C	II	6
5	Touchdown	Excessive touchdown speed or unstable touchdown	Misjudgement of touchdown status might cause excessive deviation of pitch angle and speed from specified values. With delayed handling, flight accident could occur.	C	II	6
6	Wheel-brake	Insufficient collective pitch or brake control error	Slight impact	D	IV	19

According to Table 1, human errors of highly risks are identified in the single-engine failure scenario, including delayed obstacle avoidance, errors in glide path altitude and attitude control, and misjudgment of touchdown status. Corresponding optimization recommendations were proposed accordingly as follows:

a) To enhance environmental obstacle detection during landing, timely alerts should be provided to pilots for obstacle avoidance preparation. In the event of pilot failure to identify terrain obstacles or respond promptly, the cockpit automation system should be activated to assume flight control and prevent controlled flight into terrain (CFIT).
b) To establish route plan of single-engine/auto-rotation landing, such as timely alerts to inform the pilots of excessive descent angles, abnormal touchdown speeds and angles of attack, or enhancing emergency procedure training to strengthen the pilots' compliance with operational standards.

Furthermore, pilot test evaluations were integrated to conduct ergonomic experiments in emergency scenarios, utilizing physical prototypes to validate pilot performance under specific operational conditions.

DISCUSSION

The Human Safety Assessment (HSA) methodology presented in this study is fully aligned with the ARP-4761/ARP-4754A safety assessment framework. Starting from the event-chain model, each human-related basic event is

systematically mapped to its corresponding cognitive error category (using CREAM taxonomies) and assigned a Human Error Index. By integrating this interdisciplinary human-factor safety technology into the aircraft development program, the approach establishes a reference framework for both technical requirements and implementation procedures. It consolidates a comprehensive set of work instructions spanning the entire lifecycle of human-factor safety design, analysis, assessment, and verification, explicitly defining a task-scenario and fault-logic-driven methodology for evaluating the impact of human error. This provides a structured foundation and actionable guidance for subsequent engineering activities.

To mitigate risks associated with single human error, a dedicated human error and impact analysis is conducted to identify hazardous events with human-factor contributions. Beginning with system-level fault trees derived from aircraft safety assessments, minimal cut sets (MCSs) leading to catastrophic or hazardous end states are extracted. Each basic event within these MCSs is scrutinized to determine if it could be precipitated by human action, with such events retained as focal points for subsequent analysis. The procedure is executed in two sequential stages:

Hazardous-Event Identification Based on Fault Logic

The system fault trees are traversed to isolate MCSs with top events classified as catastrophic or hazardous. Each basic event in these MCSs is then evaluated for potential human causation. For instance, the uncommand shut-off of fuel flow is a basic event in the MCS for "loss of fuel supply." This event could be initiated by the pilot's inadvertent switch actuation and is therefore prioritized for further analysis.

Human-Error and Impact Analysis Focused on Human-Related Basic Events

For each human-related basic event identified in Stage 1, the specific human-error modes that could activate and propagate to the top event are determined. Two distinct failure scenarios are analyzed:

a) Single-error induction of simultaneous MCS events—e.g., a second-order MCS comprising events A and B could be triggered by a single human error C, which directly causes both A and B. This dual activation compromises the defense-in-depth principle and precipitates a catastrophic failure.

b) Error escalation after an independent fault—e.g., if an engine fire already exists and the crews are required to isolate the affected side, an erroneous switch selection that inadvertently shuts off the healthy engine would result in dual-engine flame-out, transforming a manageable emergency into a catastrophic event.

CONCLUSION

This study proposes a systematic methodology that integrates the identification and quantification of human error into the standard aircraft system-safety analysis framework. By combining event-chain analysis with CREAM-based methodologies and conventional risk-matrix criteria,

potential human-factor-related safety vulnerabilities can be detected as early as the conceptual design phase. Furthermore, the Human Safety Assessment (HSA) approach will be expanded to address maintenance-related error prevention, thereby reducing the probability of aircraft safety incidents attributed to human errors.

ACKNOWLEDGMENT

The authors would like to thank the financial support provided by Materiel Human Factors and Ergonomics Laboratory, CAPE AVIC.

REFERENCES

Bohrey, O. P., Chatpalliwar, A. S. (2024). Mitigation of human factors in aviation maintenance. Theoretical Issues in Ergonomics Science Volume 25 No. 5, pp. 642–654.

Chen, L. J., Chang, S. N. (2011). An approach of AHP for human factors analysis in the aircraft icing accident. Procedia Engineering Volume 17, pp. 10–16.

Chen Y., Wu J., Zhu B., and Meng X., Human-factor oriented safety analysis on navigation process of ships in polar waters. Journal of Safety Science and Technology Volume 20 No. 5, pp. 27–34.

Hu J., He L., and Wang R., Review on safety evaluation of freeway interchanges. China Journal of Highway and Transport Volume 33 No. 7, pp. 17–28.

Ji, X. F., Cheng, W., and Yang, J. (2009). Evaluation model for railway human factors safety based on information extraction. Proceedings of the 2009 International Conference on Information Management, Innovation Management and Industrial Engineering (ICIII), pp. 216–218.

Ma, L. H., Ma, X. X., Lan, H., Liu, Y., and Deng, W. Y. (2022). A data-driven method for modeling human factors in maritime accidents by integrating DEMATEL and FCM based on HFACS: A case of ship collisions. Ocean Engineering Volume 266 No. 2.

Nogueira R., Melicio R., Valério D., and Santos L. (2023). Learning methods and predictive modeling to identify failure by human factors in the aviation industry. Applied Sciences Volume 13 No.6, pp. 40–69.

Perboli, G., Gajetti, M., Fedorov, S., and Lo Giudice, S. (2021). Natural language processing for the identification of human factors in aviation accident causes: An application to the SHEL methodology. Expert Systems with Applications Volume 186.

Qiao, W. L., Liu, Y., Ma, X. X., and Liu, Y. (2020). Human factors analysis for maritime accidents based on a dynamic fuzzy Bayesian network. Risk Analysis Volume 40 No.5, pp. 957–980.

Rodriguez, M. A., Bell, J., Brown, M., and Carter, D. (2017). Integrating behavioral science with human factors to address process safety. Journal of Organizational Behavior Management Volume 37 No.3, pp. 301–315.

Tian L., Bao L., Gao L., Chen Z., Zhang K., and Liu X., Human safety risk factors in daily operations of high-speed railway train dispatchers. Railway Transport and Economy Volume 46 No. 1, pp. 116–123.

Wang L., Wang J., and Liu H., Research on a safety grading and quantification analysis model for on-site operation in hydropower plants based on human factors engineering. China Rural Water and Hydropower. 2024 No.1, pp. 262–267.

Xu Z., Research on human factor safety analysis methods for digital nuclear power plants. Ph.D. dissertation, Harbin Engineering Univ., Harbin, China, 2023.

Zhao J. and Wang J., Review on human-machine interaction safety analysis of spacecraft. Spacecraft Engineering Volume 33 No.4, pp. 85–93.

Zhou, T. Q., Zhang, J. Y., and Baasansuren, D. (2018). A hybrid HFACS–BN model for analysis of Mongolian aviation professionals' awareness of human factors related to aviation safety. Sustainability Volume 10 No.12.