Assessing system safety risks in aircraft landing

Ahmed Jilaau & Gulsum Kubra Kaya

Safety and Accident Investigation Centre, Cranfield University, UK

SUMMARY

Most aviation accidents occur during the landing phase, and accidents are analysed using traditional methods, where individual system components are analysed and, as a solution, the failed component is fixed or removed from the system. This paper aims to analyse the system safety risks in the aircraft landing process by applying the System-Theoretic Process Analysis (STPA) method. STPA enabled a comprehensive analysis of the interactions between system components. The findings revealed 140 unsafe control actions, 142 loss scenarios and 67 safety recommendations for improving the landing process. This study provides an example of STPA application in aviation and valuable insights into accident prevention in the landing phase.

KEYWORDS

System Safety, STPA, Risk Analysis, Aviation, Aircraft Landing

Introduction

Over 63% of aviation accidents occur during the approach and landing phase (Flight Safety Foundation, 2017). The aircraft landing process is complex and requires consideration of the system interactions, including human and software components. However, aviation systems are often assessed using traditional safety assessment methods focusing on individual system components (Bills et al., 2023; Mogles et al., 2018).

Traditional safety assessment methods, such as Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA), are linear, focusing on individual system components. Methods like FTA and FMEA are built on the Domino model, where accidents are caused by a chain of events. However, accidents cannot be explained by a static chain of events in complex systems, focusing on system components and aiming to remove failure on the component (Kaya et al., 2021).

System-based methods are developed to address the limitations of those traditional methods. For instance, Leveson & Thomas (2018) introduced System-Theoretic Process Analysis (STPA) for hazard analysis, and Hollnagel (2012) introduced the Functional Resonance Analysis Method (FRAM) to support event analysis and risk assessment. Various research has been conducted using these methods and proved their effectiveness in the analysis (Kaya & Hocaoglu, 2020; Sujan et al., 2024).

As the system-based methods have proven their usefulness and the aviation safety management practices tend to be based on traditional methods, this study aims to revisit the landing accidents by applying STPA to analyse risks involved in the landing phase and provide safety recommendations for aviation safety professionals. The STPA application provides valuable insights into accident prevention in the landing phase.

Method

This study applied STPA to the aircraft landing process of an A320 aircraft in four steps, as described by Leveson & Thomas (2018). These include (1) defining the purpose of the analysis, (2) modelling the control structure, (3) identification of unsafe control actions (UCA), and (4) identification of loss scenarios (LS). This study applies STPA with inputs from authors' industrial and academic expertise, relevant documents (e.g., airline standard operating procedures) and research papers.

In the first step, the purpose of the analysis is identified by defining the system, system boundaries, losses, system-level hazards, and associated system-level constraints. Losses involve something of value that is unacceptable to the stakeholders, such as loss of human life or loss of property, and hazards are conditions in the system that could lead to losses (Leveson & Thomas, 2018).

The next step is to identify the system controllers and their controlled processes to create a hierarchical control structure illustrating the interactions between the controllers. This includes the control actions of the controllers and feedback that controllers receive from the controlled process (Leveson & Thomas, 2018).

In the third step, potential unsafe control actions (UCAs) that could result in hazards are identified and analysed by defining controller constraints (CC) for prevention. A control action can become unsafe either by 'not providing the control action', 'providing the control action', 'providing a safe control action too early, too late, or in the wrong order' or when 'the control action lasts too long or is stopped too soon' (Leveson & Thomas, 2018).

The final step of STPA involves determining loss scenarios by assessing the different causal factors that can lead to the UCAs and their consequences. Based on the loss scenarios, safety recommendations are then proposed for risk mitigation (Leveson & Thomas, 2018).

Results

Define the purpose of the analysis

Four losses (L) were identified in the aircraft landing process: L1- loss of life or injury to people, L2- loss of aircraft or damage to aircraft, L3- loss of or damage to objects outside the aircraft, and L4- financial loss. Next, seven system-level hazards (H) were identified by linking them to these losses and 11 system-level constraints (SC) were linked to each hazard as follows:

- H1: Aircraft deviates from stabilised approach criteria (L1, L2, L3, L4)
  SC1: Aircraft must meet stabilised approach criteria at 1000 ft.
  SC2: If the aircraft deviates from the stabilised approach criteria, a go-around procedure must be carried out.
- H2: Aircraft continues landing without clearance [L1, L2, L3, L4)
  SC3: Aircraft must obtain landing clearance from ATC before commencing landing.
  SC4: If the aircraft continues landing without clearance, ATC must detect the violation, and measures must be taken to prevent any conflicts with traffic.
- H3: Aircraft integrity is lost during landing (L1, L2, L3, L4)
  SC5: Aircraft integrity must be maintained for all conditions of the operation.
  SC6: If aircraft integrity is lost during landing, the fault should be detected, and emergency procedures should be taken to prevent losses.
- H4: Aircraft runway overrun (L1, L2, L3, L4)
  SC7: Brakes and reverse thrust must be applied upon touchdown on the runway.
- H5: Vehicle or aircraft on runway during landing (L1, L2, L3, L4)

SC8: The runway must be vacated for the landing aircraft.
SC9: If the runway is not vacated, this should be detected, and actions should be taken to prevent collision.

- H6: Communication failure between pilots and ATC (L1, L2, L3)
  SC10: Communication must be maintained between pilots and ATC.
- H7: Inadequate runway surface condition and infrastructure (L1, L2, L3, L4)
  SC11: Runway surface condition must be maintained, and all runway infrastructure, including visual and navigation lights, must be serviceable.

Model the control structure

Figure 1 illustrates the high-level control structure comprising six controllers and 18 control actions. The blue arrows represent the control actions, and the red arrows represent the feedback mechanism between the controller and the controlled process. For example, the airline is responsible for developing and implementing standards and operational procedures for flight operations. The airline, in response, receives feedback via flight crew reports and flight data monitoring programs. Similarly, the flight crew controls the aircraft and monitors the cockpit instruments, while air traffic control (ATC) provides traffic information and landing clearance to the flight crew. In the detailed control structure in Figure 2, 16 controllers and 60 control actions were identified.

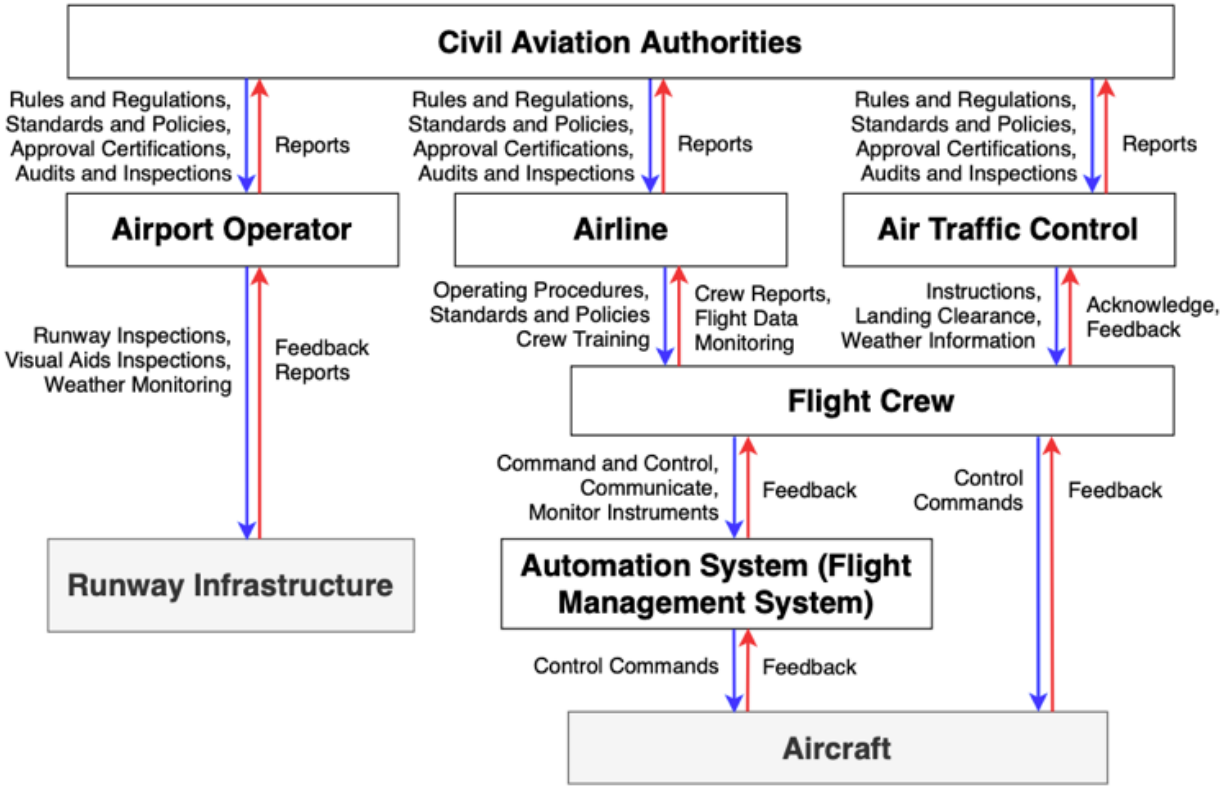

Figure 1: High-level control structure of aircraft landing process

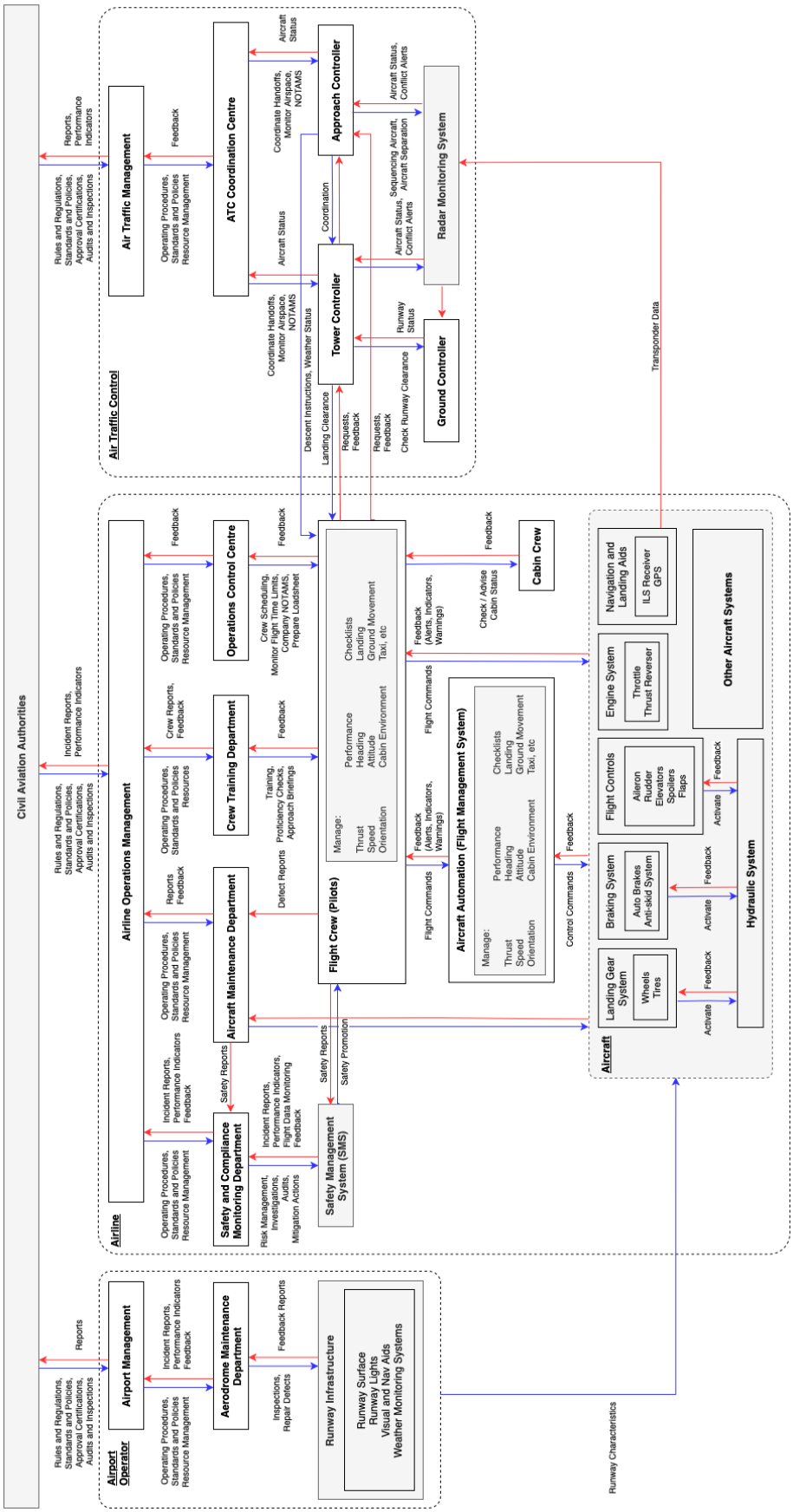

Figure 2: Detailed control structure of the aircraft landing process

Identify the unsafe control actions

In the third step, 140 UCAs were generated considering each control action by considering the four different ways (i.e., not providing the CA, providing the CA, providing CA too early, too late or wrong order, and CA stopped too soon or applied too long) a control action can be hazardous. Table 1 provides a partial list of UCAs for some key controllers.

Table 1: Partial list of UCAs

Controller and Control Actions (CA)	**Unsafe Control Actions (UCA)**
Civil Aviation Authorities: CA1.1: Develop rules and regulations	UCA1.1.1 Rules and regulations not provided by authorities UCA1.1.2 Rules and regulations provided too late by authorities
Airport Operator: CA3.1 Conduct runway inspections	UCA3.1.1 Runway inspections not carried out UCA3.1.2 Runway inspection carried out after landing
Approach Controller: CA6.2 Separation of aircraft in TMA (Terminal Manoeuvring Area)	UCA6.2.1 Separation of aircraft in TMA not provided UCA6.2.2 Separation of aircraft in TMA provided incorrectly UCA6.2.3 Separation of aircraft in TMA not maintained throughout the descent
Tower Controller: CA7.2 Issue landing clearance	UCA7.2.1 Landing clearance not issued to pilots UCA7.2.2 Landing clearance issued to pilots when runway is not clear UCA7.2.3 Landing clearance issued to pilots of wrong flight
Safety and Compliance Monitoring Department: CA10.3: Create safety awareness	UCA10.3.1: Safety awareness not carried out UCA10.3.2: Safety awareness carried out too late UCA10.3.3: Safety awareness continuously not conducted
Aircraft Maintenance Department: C11.1 Carry out maintenance inspections	UCA11.1.1 Maintenance inspections not carried out UCA11.1.2 Maintenance inspections carried out in poor working conditions UCA11.1.3 Defect not detected during maintenance inspections
Crew Training Department: CA12.1 Provide crew training	UCA12.1.1 Training not provided to crew members UCA12.1.2 Inadequate training provided to crew members
Flight Crew: CA14.1 Manage commands on FMS	UCA14.1.1 Command inputs not entered to FMS by pilots UCA14.1.2 Command input entered to FMS incorrectly
FMS: CA16.1 Adjust flight controls	UCA16.1.1 Flight controls not adjusted UCA16.1.2 Flight controls adjusted incorrectly

Identify the loss scenarios

In the fourth step, 142 loss scenarios were identified, explaining the causality of the UCAs. Based on these LSs, 67 different safety recommendations (SR) were identified to mitigate the risks in the aircraft landing process. A partial list of loss scenarios and safety recommendations is described in Table 2.

Table 2: Partial list of loss scenarios and safety recommendations

Unsafe Control Actions (UCA) and Controller Constraints (CC)	**Loss Scenarios (S) and Safety Recommendations (SR)**
UCA1.1.2: Rules and regulations provided too late by authorities (H1, H2, H3, H4, H5, H6, H7) *CC1.1.2: Authorities must provide timely rules and regulations*	S2: UCA1.1.2 might occur when adequate feedback of events not provided to authorities from the operators. This may result in existing regulations to be outdated. *SR2.1: Authorities must review oversight and regulatory audit programs and conduct risk-based audits.*
UCA3.1.1: Runway inspections not carried out (H4, H5, H7). *CC3.1.1: Airport Management must carry out runway inspections.*	S14: UCA3.1.1 might occur due to inadequate procedures related to runway inspections, resulting in FODs on runway during landing. *SR14: Airport Management must develop runway inspection procedures and provide training to staff.*
UCA6.2.2: Separation of aircraft in TMA provided incorrectly (H1, H2, H6). *CC6.2.2: Approach Controller must provide correct separation of aircraft in TMA*	S33: UCA 6.2.2 might occur if the approach controller uses inappropriate radio phraseology when communicating with pilots. *SR33.2: ATC must limit their messages to three topics to avoid confusion.* *SR33.3: ATC must provide one instruction at a time during high workload situation for pilots.*
UCA7.2.2: Landing clearance issued when runway is not clear (H2, H5). *CC7.2.2: Tower Controller must issue landing clearance to pilots when runway is clear.*	S47: UCA7.2.2 might occur if the tower controller had poor situational awareness due to feeling fatigued from increased workload. *SR47: Air Traffic Management should implement a fatigue risk management system for ATC*
UCA10.3.1: Safety awareness not carried out (H1, H2, H3, H4, H5, H6, H7) *CC10.3.1: Safety and Compliance Monitoring Department must carry out safety awareness programs.*	S63: UCA10.3.1 might occur due to inadequate safety culture within the organisation resulting in reduced safety standards. *SR63.1: Airline Management must establish safety policies to promote safety as well as fair and just culture within the organisation.*
UCA11.1.2: Maintenance inspections carried out in poor working conditions (H3). *CC11.1.2: Maintenance Department must carry out maintenance inspections in adequate working conditions*	S69: UCA11.1.2 might occur due to defective lights in maintenance hangar not being rectified, resulting in defects being missed during inspection. *SR69: Maintenance Department must ensure any deficiencies in the facilities are timely corrected to meet the standards as per the regulations and procedures.*
UCA12.1.2: Inadequate training provided to crew members (H1, H2, H3, H4, H6). *CC12.1.2: Training Department must provide adequate trainings to crew members.*	S76: UCA12.1.2 might occur due to inadequate crew training syllabus. *SR76: Crew Training Department must implement Evidence Based Training (EBT) and assess crew competencies.*
UCA14.1.2: Command input entered to FMS incorrectly (H1, H2, H3, H4). *CC14.1.2: Pilots must have correct inputs to the FMS.*	S89: UCA14.1.2 might occur if the pilot workload was high and situational awareness was low *SR89.1: Pilots must ensure there is adequate crew resource management between the crew members.*

	SR89.2: Airline Management must promote importance of performing go-arounds if the approach is unstable
UCA16.1.1: Flight controls not adjusted (H1, H3, H4). *CC16.1.1: Autopilot must adjust flight controls.*	S131: UCA16.1.1 might occur due to erroneous data from sensors on aircraft. *SR131.2: Pilots must regularly monitor / detect errors.*

Discussion

The STPA application enabled a comprehensive assessment of the aircraft landing process. The study provided 67 safety recommendations for improving safety in addition to the system level and controller constraints identified.

The findings showed that most safety recommendations were related to organisational factors, such as training, operational procedures, safety management, crew scheduling and communication, which could be due to the method as organisational factors tend to be identified more using STPA (Kaya et al., 2021). For instance, poor decision-making due to inadequate training or lack of knowledge was found to be a critical causal factor for many UCAs. With over more than 50% of aircraft accidents linked to poor decision-making by flight crew (Harris & Li, 2017), implementation of Evidence-Based Training (EBT) program for flight crew based on the guidance provided by ICAO (2013) is proposed as a key safety recommendation (SR76). This competency-based approach comprises eight main flight crew competencies, including the application of procedures, communication, aircraft flight path management– automation, aircraft flight path management – manual control, leadership and teamwork, problem-solving and decision-making, situational awareness and workload management. IATA (2024) recommends the 'application of knowledge' as an additional competence.

By considering the most likely threats to flight operation based on historical data, EBT guides airline operators to ensure the flight crew are competent to operate the flights safely. Unlike the traditional task-oriented approach of crew training, EBT promotes effective management of unexpected situations, as the lessons learnt can be utilised in various scenarios instead of pre-defined ones (IATA, 2024).

In addition, many loss scenarios, such as S89 and S92, are contributed by poor communication and ineffective task management. Based on research done by NASA, such critical factors in the cockpit account for most aviation incidents and accidents caused by human error, compared to technical issues of operating in a cockpit (Shappell et al., 2006). However, human error is a consequence, not a cause. Thus, research focused on systems to enable humans to do the right thing every time. This is also further supported by the fact that 50% of accidents and investigation reports by NTSB had mentioned Crew Resource Management (CRM) as a contributory factor, with 71% of accidents occurring during the landing phase of the flight (Wagener & Ison, 2014). As a result, CRM training for crew members has become a mandatory requirement for all commercial airlines and is a critical component of their non-technical training (Harris et al., 2024). The approach towards CRM has also evolved over the years with an additional focus on proactively identifying errors and mitigating their consequences, known as error management (Hayward & Lowe, 2017). With CRM found to be effective in improving the decision-making, situational awareness, communication, and leadership of flight crew (Salas et al., 2001), it is highly recommended that pilots ensure CRM in the cockpit is managed efficiently (SR89.1).

Furthermore, the STPA application also provided recommendations for managing unstable approaches, which were identified as a major contributing factor in 14% of approach and landing incidents, including runway excursions (IATA, 2022). One such recommendation is for airlines to implement and promote flight crew awareness of the importance of initiating a go-around when the approach becomes unstable (SR89.2). This has also been supported by a study by the Flight Safety Foundation (2017), which showed that a significant majority (83%) of runway excursions and over half of all accidents could have been avoided by performing a go-around. While there are multiple reasons why the compliance rate with the go-around policy during an unstable approach is low (3%), airlines must take measures to improve safety culture and awareness (SR63.1) among flight crew by demonstrating that the airline management will support the flight crew judgement to go-around in such scenarios without any penalty for operational disruption. Moreover, the stable approach criteria defined in the operational procedures must be regularly reviewed and updated to remove any subjectivity in their decision. The regulatory authorities must also be actively involved in improving the compliance rate for the go-around policy by reviewing the existing oversight audit programs (SR2.1) to check for go-around compliance among operators (Flight Safety Foundation, 2017).

Another key finding was the unsafe conditions created due to inadequate communication between the flight crew and ATC, as described in S33. One of the contributing factors to such misunderstanding is improper usage of radio phraseology, its speed, and language barriers, especially for non-native English speakers (EUROCONTROL, 2017). Therefore, it is essential for controllers to use the correct radiotelephony procedures as recommended by ICAO Doc444 and Doc9432 (International Civil Aviation Organization, 2007a, 2007b). Moreover, as recommended in SR33.2 and SR33.3, controllers should limit their instructions to the flight crew to three topics to avoid any misunderstanding. They must provide one instruction at a time for non-native English speakers during approach and landing where the workload is high (Barshi & Farris, 2013).

With the increase in air traffic means, air traffic control officers (ATCO) are subjected to high workload situations while managing multiple flights in airspace, resulting in scenarios such as S47. Therefore, it is highly recommended to establish an effective fatigue risk management system (FRMS) for ATCOs (SR47) in accordance with ICAO fatigue risk management guidelines to ensure adequate rest periods, rostering, and rest facilities are provided by the operator. The rostering of ATCOs should use the principles of fatigue science (International Civil Aviation Organization, 2016). A study by Li et al. (2020) found that high traffic volumes contribute to the increased mental workload of ATCOs, which contributes to more airspace incidents; hence, FRMS should focus on providing adequate breaks to maintain their cognitive resources.

While this study offers valuable insights into managing risks in the landing phase, the study has limitations. The STPA analysis could have been conducted with the involvement of subject matter experts (SMEs). This study is done as a desk study rather than involving SMEs. While this might limit the analysis, the authors used their academic and professional experience in safety science and aviation safety management.

Conclusion

STPA was applied to the aircraft landing process to examine the interactions between the various stakeholders involved and identify its system safety risks. Each controller is responsible for critical control actions, and a deficiency in a single control action could contribute to unsafe conditions. The STPA analysis resulted in a comprehensive risk analysis with the generation of many loss scenarios and safety recommendations focused on improving the system, including human and organisational factors.

References

Barshi, I., & Farris, C. (2013). Misunderstandings in ATC communication: language, cognition, and experimental methodology. In *Misunderstandings in ATC Communication: Language, Cognition, and Experimental Methodology*. Ashgate Pub. Co. https://doi.org/10.1080/00140139.2013.868633

EUROCONTROL. (2017). *European Action Plan for the Prevention of Runway Incursions (v3.0)*. https://www.eurocontrol.int/sites/default/files/2019-06/european-action-plan-prevention-runway-incursions-v3.pdf

Flight Safety Foundation. (2017). *Go-Around Decision-Making and Execution Project*. https://flightsafety.org/toolkits-resources/go-around-project-final-report/

Harris, D., Chan, W. T. K., Chatzi, A., Griebel, H., Li, W. C., Lu, T. T., McCarthy, P., Nakanishi, M., Plioutsias, T., & Ziakkas, D. (2024). Report of the working group to identify future challenges faced by the implementation of resource management in remote and distributed teams. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *14692 LNAI*, 190–200. https://doi.org/10.1007/978-3-031-60728-8_15

Harris, D., & Li, W. C. (2017). Decision making in aviation. *Decision Making in Aviation*, 1–487. https://doi.org/10.4324/9781315095080/DECISION-MAKING-AVIATION-HARRIS/ACCESSIBILITY-INFORMATION

Hayward, B. J., & Lowe, Andrew. (2017). *Safety and error management: The role of crew resource management*. 107–119. https://doi.org/10.4324/9781315181837-11

ICAO. (2013). *DOC 9995, Manual of Evidence-based Training* (1st ed.). International Civil Aviation Organization.

International Air Transport Association. (2022). *Examining Unstable Approaches-Risk Mitigating Efforts*.

International Air Transport Association. (2024). *Evidence-Based Training Implementation Guide* (2nd ed.). International Air Transport Association. https://www.iata.org/contentassets/632cceb91d1f41d18cec52e375f38e73/ebt-implementation-guide.pdf

International Civil Aviation Organization. (2007a). *Doc 4444: Procedures for Air Navigation Services - Air Traffic Management* (15th ed.). International Civil Aviation Organization.

International Civil Aviation Organization. (2007b). *Doc 9432: Manual of Radiotelephony* (4th ed.). International Civil Aviation Organization.

International Civil Aviation Organization. (2016). *Fatigue Management Guide for Air Traffic Service Providers* (1st ed.). International Civil Aviation Organization.

Leveson, N. G., & Thomas, J. P. (2018). STPA Handbook. In *2018*.

Li, W. C., Kearney, P., Zhang, J., Hsu, Y. L., & Braithwaite, G. (2020). The analysis of occurrences associated with air traffic volume and air traffic controllers' alertness for fatigue risk management. *Risk Analysis*, *41*(6), 1004–1018. https://doi.org/10.1111/RISA.13594

Salas, E., Burke, C. S., Bowers, C. A., & Wilson, K. A. (2001). Team Training in the Skies: Does Crew Resource Management (CRM) Training Work? *Https://Doi.Org/10.1518/001872001775870386*, *43*(4), 641–674. https://doi.org/10.1518/001872001775870386

Shappell, S., Detwiler, C., Holcomb, K., Hackworth, C., Boquet, A., & Wiegmann, D. (2006). Human Error and Commercial Aviation Accidents: A Comprehensive, Fine-Grained Analysis Using HFACS. *Publications*. https://commons.erau.edu/publication/1218

Wagener, F., & Ison, D. C. (2014). Crew Resource Management Application in Commercial Aviation. *Journal of Aviation Technology and Engineering*, *3*(2), 02. https://doi.org/10.7771/2159-6670.1077