Advances in Reliability, Safety and Security, Part 10 – Kołowrocki, Kosmowski (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-22-7 (printed), ISBN 978-83-68136-09-8 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Performance Based Audit Checklists Using Systemic Approach To Safety

Kateřina Grötschelová, Andrej Lališ, Natalia Guskova

Department of Air Transport, Czech Technical University in Prague, Prague, Czech Republic

Abstract

Authorities in civil aviation and other high-risk industries are currently making a progressive shift from compliance-based to performance-based oversight. This entails many challenges where among the foundational ones lies the issue of establishing effective performance-based checklists to be used when auditing organizations. This paper addresses the issue with a systemic approach to safety, namely the System-Theoretic Accident Model and Processes, which treats safety differently from its predecessors. The model is used to infer performance-based audit questions for selected type of aviation organization based on regulatory requirements, thus extending the compliance-based approach by broader reasoning about safety issues. The questions were tested with the Civil Aviation Authority during real-scale audit and the conclusions show that this is a promising approach to reduce the currently used subjective approach to evaluation of the actual performance, with many practical benefits for the Authority.

Keywords: aviation safety, compliance-based audit, performance-based audit, state safety oversight, system-theoretic accident model and processes, system-theoretic process analysis

1. Introduction

Audits are one of the essential means of safety assurance (ICAO, 2016). Although used in practice for quite some time, their preparation, execution, and evaluation may pose challenges related to audit effectiveness and efficiency. Any audit should identify the true state of affairs to enable improvements while at best, auditing well-performing systems and organizations should be limited to save resources for the systems and organizations of greater concern. These requirements demand the auditing entity to possess the necessary knowledge not only about the current legislative requirements, but also about deeper understanding of how safety works in practice. An argument could be made that this holds only for performance-based audits and prescriptive, compliance-based audits do not impose such demands on the audit team. This paper, however, takes a broader perspective, where even prescriptive audits impose such demands, although not necessary on the audit team.

In aviation state safety oversight, both approaches, i.e., compliance- and performance-based audits, are commonly used. Compliance-based audits dominate because they are easier to assure and track, while well supported by guidance materials issued by authorities (such as the European Union Aviation Safety Agency: EASA). Yet, their effectiveness remains an open issue: it is possible that a fully compliant organization may exhibit insufficient safety achievement (EASA, 2016). This is the point where the need for performance-based audits comes to the fore as they are linked to the actual safety performance. But to have an audit linked with safety performance requires a well-established performance monitoring, which brings many challenges rooted in the understanding of how safety works in practice (Sønderby, 2015). Many officials compensate for lack of guidance or clear framework on how to do this by their own skills and knowledge acquired from previous experience. This, however, leads to a rather subjective approach making an audit different depending on the audit team.

This paper addresses the above-mentioned by investigating into the current possibilities on how to prepare performance-based audit, specifically its questions to support state safety oversight in aviation. We intend to find a novel solution by means of the systemic approach to safety, which allows regulators to recognize the performance of the system as a whole, including the context, direct or indirect causes and so on (ICAO, 2021), – the most recent accident causality models and methods, of which we selected the System-Theoretic Accident Model and Processes (STAMP) (Leveson, 2012). STAMP explains safety differently from the previous safety models, which opens new ways, among other things, to audit preparation and execution. For validation purposes, the presented research was done in cooperation with the Civil Aviation Authority of the Czech Republic.

2. Materials and methods

This section describes the current state of state safety assurance focused on compliance- and performance-based audits and the new perspectives of STAMP, which are relevant to state safety assurance.

2.1. Types of audits

Two types of audits can be distinguished: compliance-based and performance-based. Depending on the need, it is possible to perform only one of them or to combine them. Both types of audits can be used to improve the audited organization. The combination of both audits can help the organization with achieving both compliance with laws and regulations, as well as effective internal processes and, eventually, satisfied customers. There is an overlap between the two audit types (e.g. both work with risks) and the process from planning to completion of both is very similar. However, they differ in how they view the organization with an impact on, for example, the preparation of the audit, the checklists, or the way the audit is executed. But both audit types aim to follow the problems found until they are resolved or until it is decided to accept the associated risks (Malsbury, 1996).

A compliance-based audit is an assessment focused on verifying compliance with policies, plans, procedures, milestones, or other predetermined requirements (Wilson and Pearson, 1994). This type of audit is rather reactive as it often identifies problems that have already occurred, and the goal of the audit is to avoid similar problems in the future. In aviation, the goal of compliance-based audits is to ensure general compliance with laws, regulations, or contracts (ICAO, 2018). Non-compliance with them can result in high financial costs for the organization, which is undesirable. During the compliance-based audit, a team of auditors reviews the documentation and possibly interviews individuals with a focus on compliance with the given procedures in the organization. The conclusion of the audit is an assessment of which requirements are met and which are not (Malsbury, 1996).

A performance-based audit is an assessment focused on the product, process, and system to determine how well they meet the customer's needs (specified and unspecified) as well as to identify opportunities for improvement (Wilson and Pearson, 1994). This type of audit, on the other hand, is more proactive because it tries to identify problems before they occur. The performance-based audit aims to improve the functioning of the organization, increase efficiency and productivity, reduce the time-consuming nature of processes, and satisfy customers. During performance-based auditing, the team of auditors should focus on comparing procedures with the reality in practice, investigating where deviations occur and why they occur. Interviews with individuals who carry out the given process or activity can also help to complete the information. The conclusions of the audit should be factual, helping managers to understand where the problem is in the system and why, highlighting processes that are good and effective (Malsbury, 1996). In aviation, this type of audit is used together with compliance-based audit, where experienced auditors also assess the performance of the organization and advise on potential problems.

2.2. System-Theoretic Accident Model and Processes (STAMP)

STAMP is a new accident causality model proposed by Leveson (Leveson, 2004). The model explains safety as a control problem unlike the older approaches where safety was considered a reliability problem (i.e. failure-oriented). The model is a foundation for several safety methods, the most popular of which are System-Theoretic Process Analysis (STPA) (Leveson and Thomas, 2018), a hazard analysis technique, and Causal Analysis based on STAMP (CAST) (Leveson, 2019), an accident analysis technique. In terms of safety assurance and audits, STPA is more relevant as it allows safety issues prediction based on system specification. The specification can be based on regulatory requirements, both prescriptive and output oriented, and predict safety issues even without operational safety data. Further, STPA and STAMP can also be used to identify appropriate safety metrics, with new ways of risk assessment. It follows that the predicted safety issues by STPA can be tied to performance measurement using the STAMP.

2.3. Audit questions based on STAMP

The methodology developed by Lališ et al., 2023 was used for creating audit questions based on STAMP in this paper. Here, the methodology was applied to the area of training organizations in cooperation with the Civil Aviation Authority of the Czech Republic, which provided practical requirements and at the same time validation during their audit in the organization.

The basis for creating audit questions based on STAMP and STPA is the control structure (the second step of STPA). For creating the control structure, regulations and other prescriptive documentation can be used, which is also used in compliance-based audits. In cooperation with the Civil Aviation Authority of the Czech Republic, the documentation Easy Access Rules for Aircrew (Regulation (EU) No 1178/2011) (EASA, 2022) was chosen for this work, according to which Authority audits training organizations. Specifically, part ANNEX VII (Part-ORA) – SUBPART GEN – GENERAL REQUIREMENTS – SECTION II – Management (EASA, 2022) was selected. Important parts necessary for the application of STPA were highlighted in the documentation (e.g. roles and processes), that were subsequently converted into a graphical form, i.e. into the control structure. Within this activity, it is useful to define losses and system-level hazards (the first step of STPA), which may affect the audited type of organization. The third and fourth steps of STPA follow after the losses and system-level hazards have been identified and the control structure prepared. From the control actions identified in the control structure, unsafe control actions and controller constraints (the third step of STPA) were created. Subsequently, unsafe control actions were explained with loss scenarios (the fourth step of STPA). This was followed by the creation of safety requirements related to loss scenarios. In addition to the safety requirements, it is also possible to create basic assumptions for the given type of organization, e.g., about how the organization should behave, achieve some goals, or meet some requirements.

Once the STPA analysis was completed, using the Lališ et al., 2023 methodology, audit questions were created. In this step, the safety requirements, and controller constraints were converted into audit questions. This formed the basis for the checklist. When creating audit questions, it is always necessary to ensure that the questions or sub-questions meet the conditions or scope of the audit. In our case, safety requirements based on loss scenarios were combined with controller constraints to provide sufficient context.

3. Results

Figure 1 shows the control structure created according to the documentation mentioned in the previous chapter (EASA, 2022). The structure consists of controllers while at the bottom, the operation of the organization represents the controlled process. The black down arrows are the control actions, and the lighter up arrows represent the feedback. The last type of relation used is coordination, which is shown by dashed horizontal lines. The entire control structure depicts how are the regulatory requirements expected to be implemented in an organization of a given type, thus the control structure can be used as a basis of the audit checklist. The questions themselves can be created by means of the STPA, specifically based on the identified safety constraints.

Table 1 shows an example of combining loss scenario-based safety requirements with controller constraints. The first column shows a loss scenario where the first part of the sentence is an unsafe control action (UCA), and the second part of the sentence is the scenario itself. The safety requirements are then listed in the second column and the third column shows controller constraints (CC). The last column includes audit questions. Loss scenario-based requirements form the basis of the question, and the controller constraints give the questions necessary context.

Table 2 shows the developed audit questions linked to the source requirements. The first two columns show respective legislative requirements, and the next the audit questions. The list of audit questions consists of one main question that defines the scope of the discussion, followed by a list of detailed questions that focus on how the organization performs a particular activity. Other columns would be added to record answers and potential finings, i.e. whether the organization *meets fully*, *partially*, or *does not meet* the respective requirement.

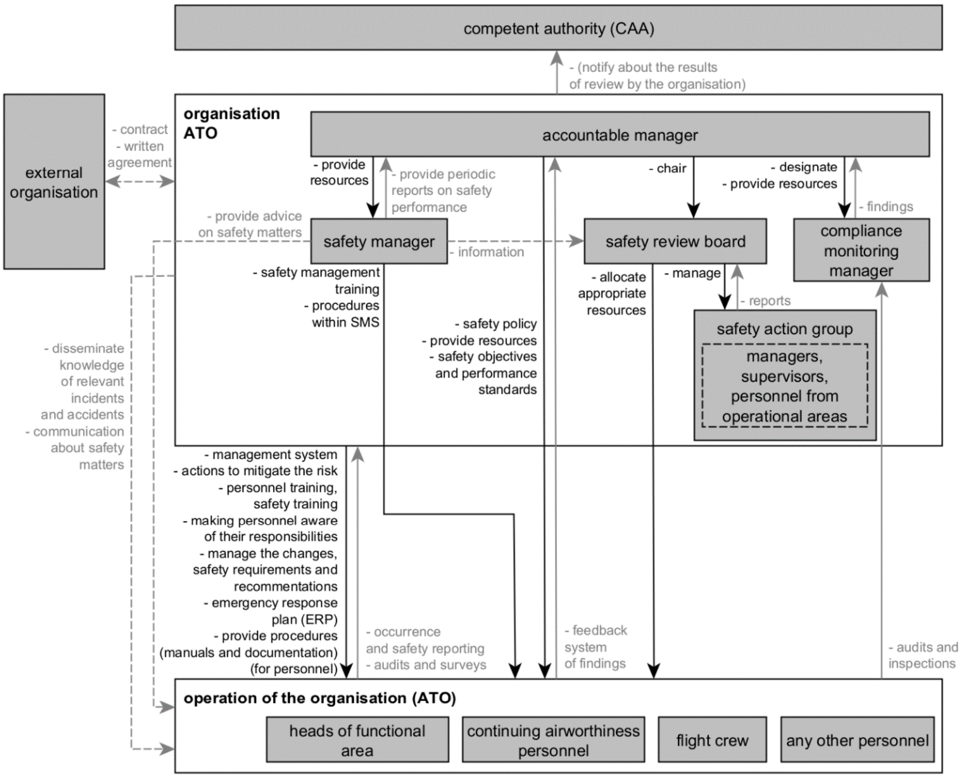
competent authority (CAA)
- (notify about the results of review by the organisation)
external organisation
- contract
- written agreement
organisation ATO
accountable manager
- provide resources
- provide periodic reports on safety performance
- chair
- designate
- provide resources
- findings
- provide advice on safety matters
safety manager
- information
safety review board
compliance monitoring manager
- safety management training
- procedures within SMS
- allocate appropriate resources
- manage
- reports
safety action group
managers, supervisors, personnel from operational areas
- safety policy
- provide resources
- safety objectives and performance standards
- disseminate knowledge of relevant incidents and accidents
- communication about safety matters
- management system
- actions to mitigate the risk
- personnel training, safety training
- making personnel aware of their responsibilities
- manage the changes, safety requirements and recommentations
- emergency response plan (ERP)
- provide procedures (manuals and documentation) (for personnel)
- occurrence and safety reporting
- audits and surveys
- feedback system of findings
- audits and inspections
operation of the organisation (ATO)
heads of functional area
continuing airworthiness personnel
flight crew
any other personnel

Fig. 1. Control structure created according to the part Management of the documentation (EASA, 2022).

Table 1. Example of converting safety requirements and controller constraints to audit questions.

Loss Scenario	Loss Scenario-Based Safety Requirement	Controller Constraint	Audit Questions
The organization is managed, but not according to the documentation [UCA-1b] because the internal processes of updating the documentation are lagging behind the practice.	Internal documentation updating processes must keep up with practice.	CC-1b The organization must be managed according to documentation.	How does internal documentation management work in the organization? Is the organization able to update internal documentation flexibly and on time?
The organization takes risk mitigation measures too late when there is a need to address the situation immediately [UCA-2c] because it is not aware of the nature of the risks.	The organization must be aware of the risk's nature.	CC-2c The organization must take risk mitigation measures on time, if immediate reaction is required.	How does the organization perform risk assessment? Is this assessment adequate given the nature of the risks it manages?
The organization requires employees to have responsibilities other than those documented [UCA-4b] because it assigns specific responsibilities only verbally and does not document them.	The organization must document all responsibilities.	CC-4b The organization shall require employees to take on only the responsibilities that are documented.	Do the documented responsibilities match the actual responsibilities of the employees in the given roles?

Table 2. Example of STAMP-based audit checklist according to the part *Management* of the documentation (EASA, 2022).

No.	Part	Audit Questions
1	ORA.GEN.200 (a) The organisation shall establish, implement and maintain a management system that includes: (1) clearly defined lines of responsibility and accountability throughout the organisation, including a direct safety accountability of the accountable manager; (2) a description of the overall philosophies and principles of the organisation with regard to safety, referred to as the safety policy; (3) the identification of aviation safety hazards entailed by the activities of the organisation, their evaluation and the management of associated risks, including taking actions to mitigate the risk and verify their effectiveness; (4) maintaining personnel trained and competent to perform their tasks; (5) documentation of all management system key processes, including a process for making personnel aware of their responsibilities and the procedure for amending this documentation; (6) a function to monitor compliance of the organisation with the relevant requirements. Compliance monitoring shall include a feedback system of findings to the accountable manager to ensure effective implementation of corrective actions as necessary; and (7) any additional relevant requirements prescribed in *Regulation (EU) 2018/1139* and in *Regulation (EU) No 376/2014* as well as in the delegated and implementing acts adopted on the basis thereof. (b) The management system shall correspond to the size of the organisation and the nature and complexity of its activities, taking into account the hazards and associated risks inherent in these activities.	Does the organization have a management system in place? • What does the management system look like in your organization and how does it work in practice? • Do you delegate any activities from the management system to external organizations? (If so, how does the management system work?) • How do you deal with introducing new or changing existing procedures within the management system? How is the time required to introduce new or change existing procedures monitored? Is the organization managed according to documentation? • How do you ensure the documentation is up-to-date? What are your procedures for this? • What aspects of the management system are included in the documentation? • How do you monitor the introduction of new or changing existing procedures when incorporated into the documentation regarding their time demands?
2	ORA.GEN.200 (a) The organisation shall establish, implement and maintain a management system that includes: (3) the identification of aviation safety hazards entailed by the activities of the organisation, their evaluation and the management of associated risks, including taking actions to mitigate the risk and verify their effectiveness;	Is the organization aware of the nature of its risks and is it taking adequate measures to mitigate them? • What are your safety risks? • How do you mitigate risks? • Show an example of a measure used to mitigate a risk. • How do you assess which risk needs to be addressed immediately and which can be addressed later?
3	ORA.GEN.200 (a) The organisation shall establish, implement and maintain a management system that includes: (4) maintaining personnel trained and competent to perform their tasks; AMC1 ORA.GEN.200(a)(4) (a) Training (1) All personnel should receive safety training as appropriate for their safety responsibilities. (2) Adequate records of all safety training provided should be kept.	Does the organization carry out regular staff training (at regular intervals, according to the current documentation)? • Are you aware which training you have to provide to your employees? Do you have a list of these trainings? • Do you have any training that you delegate to an external organization? (How do you communicate with an external organization?) • Do you carry out training according to the documentation for the given type of training? How do you monitor the currency of the training documentation? • How do you monitor the training intervals for individual employees? • Do you have materials for each training and the prescribed time required to discuss all topics? How do you ensure that everything necessary has been explained?

4	ORA.GEN.200 (a) The organisation shall establish, implement and maintain a management system that includes: (5) documentation of all management system key processes, including a process for making personnel aware of their responsibilities and the procedure for amending this documentation;	Does the organization inform employees about their responsibilities? • Do you have employee responsibilities documented? • How do you inform employees about their responsibilities? (How does a new employee learn about their responsibilities?) • Do you require employees to work outside their responsibilities? Do you inform them in advance?
5	AMC1 ORA.GEN.200(a)(3) (e) The management of change The organisation should manage safety risks related to a change. The management of change should be a documented process to identify external and internal change that may have an adverse effect on safety. It should make use of the organisation's existing hazard identification, risk assessment and mitigation processes.	Does the organization set safety requirements within the management of change to ensure safety? • How do you perform hazard analysis within change management? • How do you assess risks? • How do you set safety requirements within change management? • Show an example of a safety requirement that you have specified within change management.
6	AMC1 ORA.GEN.200(a)(3) (g) The emergency response plan (ERP) (1) An ERP should be established that provides the actions to be taken by the organisation or specified individuals in an emergency. The ERP should reflect the size, nature and complexity of the activities performed by the organisation. (2) The ERP should ensure: (i) an orderly and safe transition from normal to emergency operations; (ii) safe continuation of operations or return to normal operations as soon as practicable; and (iii) coordination with the emergency response plans of other organisations, where appropriate.	Does the organization have a defined ERP plan and does the ERP plan meet the needs of the organization? • Do you have an ERP plan in place? What does it look like? (Do you have the necessary documentation to implement the ERP plan?) • What aspects do you have listed in the ERP plan? • Have you delegated the ERP plan to an external organization? (What is the communication with the external organization and what is the related procedure?) • How do you address the introduction of new or the modification of existing procedures within the ERP plan? How do you monitor the time required to implement new procedures?

4. Discussion

This paper aimed to explore current possibilities on how to prepare performance-based audit questions to support state safety oversight in aviation. The STPA and systemic approach to safety was used as a basis for preparing the questions. The identified audit questions are based on a control structure that maps important roles, processes, and relationships between them in the audited type of organization. The control structure is based on regulatory documentation that is commonly used in today's audits. Apart from enabling the new performance-based questions, the mapping can greatly support the auditor when referring to or familiarizing with the relevant processes.

If an auditor goes into a new type of organization, they will have to apply the STPA and create a list of specific audit questions. If the STPA has already been applied to the type of organization and a list of audit questions exists, then the auditor can use the completed STPA and select only the parts that fit the scope of the audit. However, it is necessary to check the currency and possibly modify different parts of the analysis and questions to better fit the scope or the setting of the particular organization. In addition, the auditor should review the safety performance of the organization (e.g. the number of reported safety occurrences or corrective actions from previous audits) and possibly prioritize the questions accordingly.

The initial process of creating audit questions may seem demanding, however, the civil aviation authority will establish a sound basis for further audits. For example, such a basis can help auditors in the assessment of a particular organization or suggesting a solution to a problem in the organization. Among other things, this basis can also serve well new auditors who are in training and thus lack the necessary experience. With the established safety control structure, such auditors can better understand the functioning of the given type of organization.

Audit questions based on the STPA serve more for the purpose of the performance-based audits, addressing questions like *How does it work?*, *Have you ever done an activity differently and why?* or asking for practical examples etc. Considering that the audit questions in this paper were created in cooperation with the Civil Aviation Authority of the Czech Republic, there was also the idea to link the newly created audit checklist with a specific selected part of the documentation (EASA, 2022). This gives the authority the possibility to connect compliance-based audit with performance-based audit. The questions are then structured so that the auditor can ask questions in a given order according to the documentation and at the same time the questions are well connected thus forming a certain hierarchy or chain. Such a checklist is well structured for the auditor and clearly referenced to the safety control structure or safety requirements based on STAMP.

The audit checklist presented in this paper was tested during a routine audit of the Civil Aviation Authority of the Czech Republic in the organization. During the audit, the created STAMP-based questions were compared with the questions currently asked by the Authority. The organization's answers were written down and also the conclusions were compared with those of the Authority. The conclusions were found consistent and at the same time, it was found that even a person who has limited experience with auditing the given area would be able to ask and assess the organization's answers easily with the proposed checklist. Finally, the raised requirements of the audit team were included in the process creation of the checklist, thus the checklist was eventually considered suitable for future audits.

The paper gives an example from the Easy Access Rules for Aircrew (Regulation (EU) No 1178/2011) (EASA, 2022), however, the same procedure can be applied to any other legislative documentation or other type of organization. Table 2 focuses on the organization's management, but the same procedure of creating audit questions can be applied to other or more detailed parts of the documentation. The checklist of the given type of organization can also be gradually adjusted for specific organizations according to their size and scope of activity.

When planning a performance-based audit, it is advisable to generate a flow diagram of activities in the organization, identify weak areas that can cause problems, and then use the diagram to analyze unnecessary steps or, conversely, missing steps in processes (Malsbury, 1996). Although there are no flow diagrams created within the STPA, there is a control structure that can serve the purpose, as there are control actions, feedback, coordination, and organization processes. Since the next step of the STPA is the creation of unsafe control actions, we also try to find potential weak areas and explain their cause by loss scenarios. Even according to (Malsbury, 1996) it is appropriate to examine the system, which is a goal the STPA can well serve.

5. Conclusion

This paper provides a proposal for the creation of checklists for performance-based audits, based on the STAMP accident causality model. The paper described the methodology for preparing audit questions, which were organized into a checklist table. The regulatory documentation, which is part of a compliance-based audit, was divided into parts that are numbered in the table. Each numbered part of the documentation was assigned a related set of audit questions. The set of questions was tested with the Civil Aviation Authority of the Czech Republic. The results showed that the questions are well usable within the performance-based audits and correspond to the questions asked by experienced auditors for the given audited area.

A limitation of creating STAMP-based audit questions is that the systemic approach is currently not used in aviation state safety oversight, so authorities may initially have a problem with training their employees. Also, the validation process of the checklist was limited, as it was only tested on a few cases. For better validation, it is advisable to validate the checklist through several audits in different organizations.

In addition, it will be necessary to further focus on the part of the checklist that deals with the recording of the answers and their assessment. Our evaluation showed that for the needs of performance-based audit, the current form using *meets fully, partially, or does not meet* categories is insufficient for the purpose. Especially important is to focus on the *meets partially* category, because it may include both small findings that need to be corrected and more significant findings, e.g. need for implementation of an entire process into operation. It is therefore necessary to further define how an auditor should do such an assessment.

The result of this paper will contribute to supporting auditors in executing performance-based audits. It will help them to understand the processes of the organization and can be supportive in the assessment of the audit. STPA brings a new, systemic perspective to the state safety oversight process which can help to better explain some of the state safety oversight issues.

Acknowledgements

This work was supported by the grant No. CK01000073 "Digitalization of integrated aviation safety oversight" funded by the Technology Agency of the Czech Republic.

References

European Union Aviation Safety Agency (EASA). 2016. Practices for risk-based oversight. EASA.

European Union Aviation Safety Agency (EASA). 2022. Easy Access Rules for Aircrew (Regulation (EU) No 1178/2011). EASA.

International Civil Aviation Organization (ICAO). 2016. Annex 19 – Safety Management, Second Edition. ICAO, Montréal, Quebec.

International Civil Aviation Organization (ICAO). 2018. Doc. 9859: Safety Management Manual (SMM), Fourth Edition. ICAO, Montréal, Quebec.

International Civil Aviation Organization (ICAO). 2021. Doc. 10151: Manual on Human Performance (HP) for Regulators, First Edition. ICAO, Montréal, Quebec.

Lališ, A., Grötschelová, K., Stojić, S. 2023. Methodology for using the theory of STAMP safety model by the Civil Aviation Authorities.

Leveson, N. 2004. A new accident model for engineering safer systems. Safety Science 42, 237-270.

Leveson, N. 2012. Engineering a Safer World: Systems Thinking Applied to Safety. The MIT Press, Cambridge, Massachusetts.

Leveson, N., Thomas, J. 2018. STPA Handbook. [Online] http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.

Leveson N. 2019. CAST Handbook: How to learn more from incidents and accidents. [Online]. Available: http://psas.scripts.mit.edu/home/get_file4.php?name=CAST_handbook.pdf.

Malsbury, J.A. 1996. Performance Based vs. Compliance Based Auditing: The Similarities and the Differences. Princeton, New Jersey.

Sønderby, K. 2015. How can aviation regulators retain effectiveness in a performance-based environment? Lund University, Sweden. [Online]. Available: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8309632&fileOId=8309639

Wilson, P.F., Pearson, R.D. 1994. Performance-Based Assessments: External, Internal, and, Self-Assessment Tool for Total Quality Management. ASQ Quality Press.