International Journal of Safety Science
Vol. 02, No. 01, (2018), pp. 84-93
DOI:10.24900/ijss/02018493.2018.0301

Special Issue Article: The 5th European STAMP Workshop (ESW) 2017, Chief Editor: Svana Helen Björnsdottir, Reykjavik University

Documentation of Assumptions and System Vulnerability Monitoring: the Case of System Theoretic Process Analysis (STPA)

Nektarios Karanikas

Aviation Academy, Faculty of Technology, Amsterdam University of Applied Sciences
n.karanikas@hva.nl, nektkar@gmail.com

Abstract

The documentation of assumptions during hazard and risk analysis allows the monitoring of their validity which can function as a leading performance indicator. This paper through a combination of literature references and pragmatic standpoints presents the groups of assumptions which the analyst can make at each discrete step of the System Theoretic Process Analysis (STPA) and elaborates on the connection between invalid assumptions and system vulnerability. Ten assumption groups were identified as possible during the performance of STPA, starting from the system definition and moving to the last activity of the particular technique, namely the generation and testing of causal scenarios. The assumptions were attributed to the boundaries with regard to the scope and resources of the analysis and the inevitable assignment of maintenance of constraints and fulfilment of requirements to agents that are external to the system under study. Also, the impact of the assumptions was linked to the hierarchical system level under the claim that the higher the system level the assumptions are made, the higher the system vulnerability. The assumption groups derived in this study can assist users of STPA and other hazard analysis techniques in the recognition and documentation of assumptions and render their analysis results more credible and transparent. Moreover, the current work might complement hazard analysis guidelines and can be incorporated in software applications that support such analyses.

Keywords: *hazard analysis; assumptions; STPA*

1. Introduction

1.1 Documentation and validation of assumptions

Assumptions are an inextricable part of problem-solving due to our limited knowledge, capacity and resources, in general, to fully comprehend, exert control over everything that surrounds a problem and completely ensure that our solutions will sustain any external or internal disturbance. The more the assumptions an analyst makes, the higher the dependency on agents and factors outside our direct control; thus, the validity of the assumptions is of paramount importance to claim viability of any solution. Benjamins, Fensel, & Straatman [1] supported that in problem-solving there is the law of conservation of assumptions, which the authors classified as ontological and teleological. Ontological assumptions regard to the gap between the problem of concern and the domain knowledge available, and teleological assumptions refer to the distance between the original goal and the real functionality offered by the solution. Benjamins, Fensel, & Straatman [1] argued that complexity in problem-solving is reduced by introducing either more ontological assumptions, which require fewer teleological ones, or more teleological assumptions, which then lead to making fewer ontological ones. The premise is that for a

given goal, each problem-solving approach will have the same total number of teleological and ontological assumptions.

The challenges around assumptions have concerned researchers as well as analysts across various industry sectors and business domains. Hwarng, Chong, Xie, & Burgess [2] in their work on a real supply chain incorporated a multi-level and multi-retailer model and showed that an oversimplification of assumptions about various parameters in complex environments could distort the outcomes of analyses. As Hwarng, Chong, Xie, & Burgess [2] concluded, the difference between reality and simplification, the latter leading to assumptions, reflects the difference between observed and expected performance respectively. Harkleroad, Vela, Kuchar, Barnett, & Merchant-Bennett [3] in their report about the NextGen concept's assessment and validation recognised that simplifying assumptions might lead to masking potential unsafe scenarios. Verdolini, Anadon, Lu, & Nemet [4] in their study regarding the elicitation of expert's judgment about the future costs of photovoltaics indicated assumptions related to the future public research & development investment, discount rates, and technological changes over time. Verdolini, Anadon, Lu, & Nemet [4] suggested an improved design of elicitation techniques, a careful selection of experts and interpretation of results due to the high levels of biases, which are reflected on the assumptions each expert makes.

Furthermore, Wang & Chen [5] detected that fundamental assumptions used in multi-zone airflow network models in building (i.e. the uniformity of zone air temperature and contaminant concentrations, and air momentum effects) could be invalid in three scenarios and could cause significant calculation errors and flawed designs. Tong [6] recognised that conservative assumptions in the estimation of material fatigue strength of aircraft structures count, amongst others, for the variability of the operating environment, but do not consider the cumulative operating damage, and assume a statistical independence of load and strength, which might not always be valid. As Tong [6] noticed, the validity problem when using probability distributions becomes bigger when data is unreliable, unavailable or scarce and, consequently, calculations lead to inaccurate risk assessments.

Various professional and academic literature mentions that analysts must visibly document all assumptions, and, in principle, assumptions refer to the conceptual and analytical models used to illustrate the relationships and behaviours of system elements along with the surrounding conditions and the quality of available data [3, 7-14]. The factors above will determine the fidelity of risk analyses underpinning the decision-making throughout the life cycle of products and services. The documentation of the corresponding assumptions will allow their future validation even when those are based on conservative best estimates. Most of the safety assessment methods listed by Everdij & Blom [15] are based on assumptions about the state of systems and behaviour and relationships of their parts, and some methods identify the need to document, check and revise risk assessment results based on real world data [e.g., Adaptive Control of Thought-Rational (ACT-R), Comparative Safety Assessment (CSA), Goal Structuring Notation (GSN), Traffic Organization and Perturbation Analyzer (TOPAZ)]. Guidelines of various domains also mention the validation of assumptions. For example, in enterprise risk management the assumptions underpinning the business objectives must be checked [16], in industrial safety a comparison of current system with the design assumptions must be a process of a management system [8], and in life cycle cost analysis the assumptions behind numerical figures must be periodically validated [17].

An example of an extensive reference to the mandate for clear documentation and validation of assumptions is the work of Masson, Morier, & FAST [18]. The same authors in their technical report about a methodology to assess upcoming risks in aviation mentioned the necessity to explicitly document the assumptions of current, transitional and future operations. They also stressed out the mandate to collect and evaluate all

assumptions to picture the uncertainties related to lack of knowledge about future systems and the variability of relevant parameters. Masson, Morier, & FAST [18] also accepted that in reality, such assumptions are inevitable in the attempt to simplify the inherently complex aviation system and derive workable solutions for particular scenarios; nevertheless, a clear documentation and justification of the assumptions made must accompany every risk assessment work.

However, literature does not always seem addressing the need to validate assumptions consistently. For instance, the US Air Force [19, p. 124], in its 125-pages long document about risk management guidance and tools, refers only once to the need to explain the assumptions underlying the methodology used to estimate residual risk. Another example given, the Safety Management International Collaboration Group [20, p. 15] mentions only once the requirement for documentation of the assumptions linked to risk-based decision making. None of these two documents refers to the validation of assumptions. Leveson, Wilkinson, Fleming, Thomas, & Tracy [21] also indicated a lack of documented assumptions in the risk assessment conducted with the Aerospace Recommended Practice (ARP) 4761 [22] for a wheel brake system. This fact did not allow the authors to understand its operation fully, and the information included in the analysis seemed to assume that pilots would be fully and always capable of dealing with any failure. Similarly, McLeod [23] articulated that the assumption that skilled and competent people will respond as expected and according to the training provided seems prevalent in risk assessments but not explicitly stated.

1.2 Assumptions and vulnerability

Acknowledging the effects of invalid assumptions on system performance, Leveson [24] proposed an approach to move beyond the traditional likelihood-severity practice in risk assessment and relate the vulnerability of sociotechnical systems to the extent to which the assumptions underlying the design, production and operation of systems are maintained during their lifetime. Such assumptions could be linked to the adequacy of hazard analysis and the design, construction and implementation of mitigation controls, changes over time such as new hazards, degradation of controls, diversity of operating environments, behaviour of system components, and the operation of an effective and mature safety management [24]. The author above pointed out that the documentation of assumptions is an essential prerequisite that will allow the monitoring of their validity. Furthermore, assumptions can be also associated with the likelihood-severity themselves. In alignment with the observations of Leveson [24] that the consideration of likelihood might lead to flawed decisions in risk management, Sagan [25, p. 943] had noticed that organizations "…too easily wash out estimates of low-probability events by transforming them into assumptions of impossibility" and exclude the respective eventualities from their contingency plans.

According to Leveson [24], the main assumptions during a system's deployment is that the decisions made during design are correct, that the system will be constructed, operated and maintained as designed, and that operators will respect the system limitations. These assumptions might render a system susceptible to several hazards and can be generated at any analysis stage, even when using a systematic technique, such as the System Theoretic Process Analysis (STPA) [26]. A complete analysis with STPA will ideally reveal all known parameters affecting system performance to allow the development of causal scenarios and, afterwards, an evaluation of system vulnerability. However, from a pragmatic standpoint and taking into account that no one is fully knowledgeable of and has control over open systems, assumptions will unavoidably be part of the STPA analysis itself [e.g., 27]. This paper describes the groups of assumptions which the analyst might make during the application of STPA, and then discusses the monitoring and possible effects of assumptions. The author of this paper did not find in literature any

references about the types of possible assumptions during the application of other analysis techniques such as the Failure Mode and Effects Analysis (FMEA) and Hazard and Operability studies (HAZOP). Therefore, the author envisages that a similar approach will be of merit for any hazard analysis technique to facilitate analysts in detecting and documenting their assumptions, and, consequently, offering the opportunity for their monitoring.

2. Assumptions within STPA

The specific section refers to the groups of implicit or explicit assumptions that analysts can make during the application of STPA and it is structured according to the STPA steps [26]. Within each of the following subsections, the author explains the parameters and literature linked to assumptions per STPA activity and describes each generic assumption category in italics. The author would like to note that (1) the assumption groups stated hereby do not refer to the quality of the execution of STPA (e.g., inclusiveness of control actions or context variables, exhaustiveness of causal factors) but to the output of each analysis task, and (2) STPA is an iterative process, hence every assumption made at early analysis stages might be revisited during several analysis iterations.

2.1 STPA preparation steps

2.2.1 System definition

The first task of the analyst is to define the system under study, meaning the spatial, temporal and interaction boundaries of the system according to the scope of the analysis. The decision about the elements and links to be included in the analysis means that, under the reality of open systems, there are external influences and changes over time that the analyst assumes to be controlled or negligible. As literature suggests [e.g., 28-31], all socio-technical systems are dynamic in nature and interact with each other. The viability and sustainability of a system depends on the degree to which it can adapt timely and successfully to changing environments. Therefore, the two groups of assumptions mentioned below are made in the phase of system definition/analysis scope: the elements and interactions excluded from the analysis, where applicable:

- *have predictable effects on the system under study (Assumption group No 1)*
- *change at a pace that allows a successful adaptation of the system under study to maintain achievement of its objectives (Assumption group No 2)*

2.2.2 System accidents and hazards

The system objectives included in the analysis will drive the definition of system accidents. Originally STPA was introduced to improve safety and the majority of the published studies and research focus on safety related objectives[1]. However, various authors have claimed and partially demonstrated that the specific technique can be applied to any business objective, such as quality, producibility, security etc. [e.g., 32-33]. Therefore, the selection of a specific set of concurrent system objectives to be included in the STPA analysis leads to the assumption that those can be met in parallel to the objectives excluded from the analysis. This selection leaves a window for conflicting goals that can result in underperforming systems and catastrophic events [34-35]. The author would like to clarify that the achievement of concurrent goals does not always mean a conflict amongst those. A clash can happen when the capacity of the controller and the resources available do not suffice to meet all goals in parallel, or when different goals require oppositely directed actions and decisions.

For example, albeit several authors have approached the relationship between safety and security in terms of commonalities and differences as well as opportunities for their

[1] http://psas.scripts.mit.edu/home/

synergy [36-38], the reality is that often those two system objectives can be antagonistic [39]. If both safety and security outputs are included in a STPA analysis as system objectives, then the analyst will detect possibly conflicting areas and will generate suitable requirements from STPA. In the opposite case, safety and security might conflict at an extent that renders the system vulnerable to unsafe conditions inflicted by one or both of these objectives. The third group of assumptions can be described as follows:

The system objectives included in the analysis do not conflict with the system objectives excluded from the analysis (Assumption group No 3)

2.2.3 System constraints

Following the definition of system accidents and hazards, the analyst will derive the system constraints. The maintenance of some of the constraints might not depend solely on the system controllers, might fall out of the responsibility of the sponsor of the study or might not be considered due to lack of expertise and knowledge of the analysts. In those cases, the responsibility to maintain such system constraints lies with external agents. The fourth assumptions group can be expressed as follows:

The agents outside the system under study maintain the system constraints assigned to them (Assumptions group No 4)

2.2.4 Control structure

The control structure can include different levels of decomposition, each of these including substructures of the system and respective control loops. Although not explicitly stated in the theoretical foundation of STPA [26], the system decomposition will stop at the level to which the analyst can predict with confidence the behaviour of elements. This presumes that these elements consist of relatively simple electromechanical parts and function independently from human or software inputs. However, the resources devoted to the analysis, the scope of the study and the level to which the behaviour of system parts is trusted will actually drive the analysis depth. Thus, there can be cases that analysis will stop before reaching the lowest required level of decomposition, this leading to the fifth group of assumptions:

The behaviour of elements and/or subsystems belonging to system levels lower than the ones analysed can be confidently predicted (Assumptions group No 5)

2.2 STPA step 1

The listing of Unsafe Control Actions (UCA) will lead to the formulation of requirements that the respective human or software control shall maintain. These requirements shall be part of the control algorithm of the corresponding human or software controllers. The assumption is that controllers have the capacity to execute the corresponding actions. Since the causal factors to be generated in the next STPA step address reasons that render humans and/or software unable to maintain the constraints related to UCA, the author considers the current analysis step as transitional and not incorporating assumptions.

2.3 STPA step 2

2.3.1 Causal factors

The specific step regards the derivation of causal factors linked to either the execution of UCA within various contexts or the ineffectiveness of control actions (CA) executed when the context is appropriate. The types of causal factors leading to UCA can be categorised as follows:

1. Poor quality of applicable requirements, objectives, rules etc.

2. Controller's unawareness or misperception of requirements, objectives, rules etc.
3. Inadequate information flow from other controllers in terms of timeliness and quality
4. Inadequate feedback from the sensors to the controller in terms of timeliness and quality
5. Inadequate information flow between process and sensor(s) in terms of timeliness and quality

,and the types of causal factors leading to ineffective CA can be categorised as follows:

6. Poor quality of CAs execution in terms of speed, force, direction etc. (see also [40]).
7. Misbehaviour of actuators transmitting the CAs
8. Misbehaviour of process parts executing the CAs
9. Conflicts with other controllers
10. Inadequate resources for the execution of the CAs
11. Unforeseen or uncontrolled disturbances
12. Adverse impact of process on system state, objectives etc.

Typically, each of the causal factors generates a requirement which for the factors No 1, 3-5, 7-10 and 12 listed above refers principally to agents outside the system under study (e.g., authorities, other controllers, system designer and manufacturer). This case is similar to assumption group No 4 (section 2.2.3), but now it refers to the lower level of system requirements. Factor No 11 relates to the external disturbances that the system can tolerate, which actually are reflected in the assumption groups No 1 & 2. Concerning causes No 2 and 6, the requirements refer either to the process controller, under the notion of personal responsibility of human controllers, or external agents. The latter shall ensure the technical capability of software controllers or the proper selection, training, information provision, working environment conditions etc. regarding human controllers.

For example, the fulfilment of a general requirement for factor No 1 (e.g., adequate quality of procedures) lies on a higher-level controller. Alike, the designer and the system manufacturer/developer must meet the requirement for timely and high-quality feedback from the process to the sensors (i.e. to counteract causal factor No 5). On the other hand, the correct execution of a CA (i.e. requirement from factor 6) depends partially on the controller (e.g., own responsibility to keep physically and mentally fit) or other agents (e.g., effects of the duration of working shifts scheduled by the employer, training provided). Based on the above, the following assumptions will remain after completing STPA step 2:

External agents will fulfil the requirements assigned to them (Assumptions group No 6)

The system controllers will fulfil the requirements assigned to them given that external agents will have fulfilled their relevant requirements (Assumptions group No 7)

2.3.2 Causal scenarios

Finally, the list of causal factors allows the analysts to generate and then test causal scenarios to evaluate the effects of various combinations of causal factors for given contexts. Although STPA will lead to a complete set of causal scenarios, possible limitations can apply to scenario testing (e.g., amount of time and resources invested, availability and validity of test instruments, sample size). Hence, it can occur that some scenarios will not be checked, at least at the same time, some requirements cannot be tested within each scenario, or the test results have inadequate validity and reliability. Such limitations might mostly apply when requirements regard non-technical requirements such as human performance levels, quality of documentation and procedures, quality of verbal communication etc. due to the high variability expected across different populations and over time.

An illustration of the limitations of causal scenario testing is the case Holt & Fisher [41] presented and regarded several cases with unexpected main landing gear collapses during taxiing, take-off and landing. Following the first events, the investigation team performed extensive checks of the specific system's operation and components' integrity but they did not detect any failures or problems. Those tests, in the language of STPA, can correspond to the checking of individual requirements sourcing from different causal factors. Based on the results of these initial checks, there were engineering voices that viewed the uncontrolled collapse of main landing gears as practically improbable, although the reality had shown differently. The judgment of those engineers could have stopped the investigation at the level of testing individual requirements and not examining the behaviour of the system as a whole (i.e. complete causal scenario). However, the firm interest of the stakeholders involved and the persistence of the investigators in conjunction with a newer occurrence led finally to the assembly of a full-scale system mounted on a test rig. This allowed the execution of tests under various combinations of vibration levels, voltage signals, hydraulic pressures, tyres balance etc. Such scenarios with dynamic conditions had not been tested during the original development of the main landing gear system, but Holt & Fisher [41] did not mention whether these scenarios had been contemplated but not checked for various reasons. Only after 70 testing runs under conditions similar to the ones of the occurrences, the landing gear collapsed, revealing findings that led to the formulation of safety recommendations. If the investigators had stopped the trials after the 69th attempt, the specific problem would be probably still remain unexplained. The case described above reflects the following groups of assumptions that can apply to the operationalisation phase of STPA step 2 outputs:

The occurrence of causal scenarios not to be tested is practically improbable (Assumptions group No 8)

The requirements excluded from scenario testing are always fulfilled (Assumptions group No 9)

The results from causal scenario tests are reliable and valid (Assumptions group No 10)

3. Discussion

The ten categories of assumptions formulated in section 2 above are related to each of the analysis steps included in STPA, and they were derived through a logical argumentation, review of relevant literature and the author's experience in hazard analysis in general and application of the particular technique. According to the argumentation presented in section 2 above, the reasons leading to assumption groups No 1, 2, 5, 6, 7 and 10 will be always present during STPA analysis, whereas the extent to which assumptions categories No 3, 4, 8 and 9 will apply depends on the scope and resources of the analysis and its exploitation. Referring to the classification of Benjamins, Fensel, & Straatman [1], it seems that the assumption groups No 3, 4, 6-7 and 9 can be categorised as purely teleological, whereas the assumptions belonging to the rest of the groups can be ontological or teleological depending on the underlying reasons. Thus, without knowledge about the factors driving the acceptance of the assumptions, the claim of Benjamins, Fensel, & Straatman [1] about the summation of assumptions to the same total number per system/case cannot be checked.

It is noted that the final number of assumptions will be determined according to the characteristics of the system under study (e.g., number of elements, levels and connections) and the degree and phase of its analysis (e.g., early design stage or existing system). For instance, the number of assumptions of group No 3 will equal to the number of system objectives excluded from the analysis. Similarly, the number of external agents that are (co)assigned to the maintenance of constraints or fulfilment of requirements will drive the number of assumptions falling in the categories No 4 and 6 respectively. As the

author mentioned earlier in section 2, the analysts will revisit and revise all assumptions several times during the analysis.

The impact of assumptions concerned, Leveson [24] pointed out that each system has its unique design and respective assumptions and the invalidity of the latter might render the system unsafe. Extending the specific viewpoint, when referring to higher levels of control structures, unavoidably some assumptions will apply to various subordinate systems and their invalidity could threaten multiple subsystems. For example, the correct design and effective implementation of a safety management system within an organisation can be an assumption affecting the performance of many socio-technical subsystems (e.g. individual operating units), and the adequate quality of a State safety program might be an assumption linked to various subordinate organisations. Therefore, it can be argued that the vulnerability of systems due to invalid assumptions [24] increases with the hierarchical level to which the assumptions are referred; the higher the hierarchical level the assumptions are invalid, the higher the vulnerability of the system.

The above view is complementary to the notion of critical assumptions that, according to risk management literature [e.g., 42], are the ones with the highest degree of uncertainty. Such an uncertainty is even higher when assumptions are made in the early design phase of a system. It is clarified that the author of this paper recognises that the assumptions closer to the level of physical processes might be crucial too for the given system, but such assumptions will affect performance more locally even under the reality of side effects. Thus, when considering the STPA steps and their respective assumptions, the ones to be generated earlier in the analysis will have larger effects than the assumptions made at lower analysis levels. For instance, the assumptions related to the flight of a specific aircraft type operated by a particular company might affect the operations of this company and its related stakeholders, but the assumptions linked to the design of the specific aircraft type will influence the global fleet and a larger population.

4. Conclusions

This paper presented the assumptions researchers and practitioners might make while performing a hazard analysis with STPA, either for existing systems or during the design phase, and exploiting its outputs per analysis step. The results of this work were based on a specific line of reasoning grounded in literature and practice. The assumption groups generated aims at raising the awareness of analysts about possible and inevitable "imperfections" of any analysis, and demonstrate that even system-focused and systematic analysis techniques such as STPA can be still subject to assumptions.

Considering that literature recognises that the validity of assumptions comprises a crucial feedback mechanism as a means to adjust a system to new conditions or even proceed to its redesign, the author prompts hazard analysts to contemplate the categories of assumptions suggested in this paper and explicitly document their assumptions. Certainly, the assumption groups proposed can be subject to amendment based on further experience and perspectives of other analysts as well as future research. Future publications can focus on specific examples of the assumptions generated during system analysis and validate the inclusiveness of the assumption groups presented in this study. Nevertheless, any honest effort for designing, building and operating safe systems shall be in the direction of generating the least possible assumptions.

Also, under the fact of limited resources, the author suggests the monitoring of assumptions validity under a top-down system level priority, an approach that could also drive the development of respective leading indicators. Lastly, a consistent and transparent documentation of assumptions is expected to increase the credibility of hazard analyses. Therefore, regarding especially STPA, it is suggested to consider the inclusion of a dedicated section about analysis assumptions in the next versions of STPA

application guidelines. Also, it is proposed to examine the incorporation of respective fields in the software packages supporting the application of STPA [e.g., 43-45].

Acknowledgments

The author wants to express his appreciation to Dr Maria Mikela Chatzimichailidou, Mr Martin Rejzek and Mr Anastasios Plioutsias for their comments on a preliminary version of this work.

References

[1] R. Benjamins, D. Fensel and R. Straatman, "Assumptions of Problem-Solving Methods and their Role in Knowledge Engineering," in Proceedings of the 12th European Conference on Artificial Intelligence, 1996.

[2] H. B. Hwarng, C. S. P. Chong, N. Xie and T. F. Burgess, "Modelling a complex supply chain: understanding the effect of simplified assumptions," International Journal of Production Research, vol. 43, no. 13, pp. 2829-2872, 2005.

[3] E. Harkleroad, A. Vela, J. Kuchar, B. Barnett and R. Merchant-Bennett, "Risk-based Modelling to Support NextGen Concept Assessment and Validation, Report ATC-405," Massachusetts Institute of Technology, Cambridge, MA, 2013.

[4] E. Verdolini, L. D. Anadon, L. Lu and G. F. Nemet, "The effects of expert selection, elicitation design, and R&D assumptions on experts' estimates of the future costs of photovoltaics," Energy Policy, vol. 80, p. 233–243, 2015.

[5] L. L. Wang and Q. Chen, "Evaluation of some assumptions used in multizone airflow network models," Building & Environment, vol. 43, pp. 1671-1677, 2008.

[6] Y. C. Tong, "Literature Review on Aircraft Structural Risk and Reliability Analysis," DSTO Aeronautical and Maritime Research Laboratory, Melbourne, 2001.

[7] AFSC, Air Force System Safety Handbook, Kirtland, US: Air Force Safety Centre, 2000.

[8] D. McDonald, Practical Industrial Safety, Risk Assessment, and Shutdown Systems, Oxford: Elsevier Science & Technology Books, 2004.

[9] A. I. Glendon, S. G. Clarke and E. F. McKenna, Human Safety and Risk Management, 2nd ed., Florida, US: CRC Press, 2006.

[10] P. White, "Review of Methods and Approaches for the Structural Risk Assessment of Aircraft, DSTO–TR–1916," Defence Science and Technology Organisation, Air Vehicles Division, Department of Defence, Australia, 2006.

[11] G. Yang, Life Cycle Reliability Engineering, New Jersey: Willey & Sons, 2007.

[12] NASA, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA/SP-2011-3421, 2nd ed., Washington: National Aeronautics and Space Administration, 2011.

[13] D. Smith, Reliability, Maintainability and Risk: Practical Methods for Engineers, 8th ed., Oxford: Butterworth-Heinemann, 2011.

[14] DOD, System Safety, MIL-STD-882E, US: Department of Defence, 2012.

[15] M. H. C. Everdij and H. A. P. Blom, "Safety Methods Database. Version 1.1," 2016. [Online]. Available: http://www.nlr.nl/documents/flyers/SATdb.pdf.

[16] AIRMIC, Alarm and IRM, A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000, United Kingdom: The Association of Insurance and Risk Managers & The Public Risk Management Association & The Institute of Risk Management, 2010.

[17] M. Davis, R. Coony, S. Gould and A. Daly, Guidelines for Life Cycle Cost Analysis, vol. Land and Buildings, California, US: Stanford University, 2005.

[18] M. Masson, Y. Morier and FAST, "Methodology to Assess Future Risks, Action EME 1.1 of the European Aviation Safety Plan (EASp)," European Aviation Safety Agency, Cologne, 2012.

[19] USAF, "Risk Management Guidelines and Tools, Air Force Pamphlet 90-803," United States Air Force, 2013.

[20] SMICG, "Risk Based Decision Making Principles," Safety Management International Collaboration Group, 2013.

[21] N. Leveson, C. Wilkinson, C. Fleming, J. Thomas and I. Tracy, "A Comparison of STPA and the ARP 4761 Safety Assessment Process, MIT PSAS Technical Report, Rev. 1," Massachusetts Institute of Technology, Cambridge, MA, 2014.

[22] SAE, "ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," SAE International, 1996.

[23] R. McLeod, "Barrier management and its place in understanding risk," The Ergonomist, pp. 14-15, Mar-Apr 2017.

[24] N. Leveson, "A Systems Approach to Risk Management Through Leading Safety Indicators," Reliability Engineering & System Safety, vol. 136, pp. 17-34, 2015.

[25] S. D. Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security," Risk Analysis, vol. 24, no. 4, pp. 935-946, 2004.

[26] N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, Cambridge, MA: MIT Press, 2011.

[27] A. A. Adesina, Q. Hussain, S. Pandit, M. Rejzek and A. M. Hochberg, "Assessing the Value of System Theoretic Process Analysis in a Pharmacovigilance Process: An Example Using Signal Management", Pharmaceutical Medicine, vol. 31, pp. 267-278, 2017.

[28] J. Rasmussen, "Risk Management in a Dynamic Society: A Modelling Problem," Safety Science, vol. 27, pp. 183-213, 1997.

[29] J. Carroll, N. Dulac, N. Leveson and K. Marais, "Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems," Organization Studies, vol. 30, no. 2-3, pp. 227-249, 2009.

[30] S. Dekker, Drift Into Failure, UK: Ashgate, 2014.

[31] E. Hollnagel, Safety-I and Safety-II: The Past and Future of Safety Management, UK: Ashgate, 2014.

[32] W. Young and N. Leveson, "An Integrated Approach to Safety and Security Based on Systems Theory," Communications of the ACM, vol. 57, no. 2, pp. 31-35, February 2014.

[33] N. Leveson, Engineering a Safer and More Secure World, Cambridge, MA: Massachusetts Institute of Technology, 2017.

[34] E. Hollnagel, D. D. Woods and N. C. Leveson, Resilience engineering: Concepts and precepts, Aldershot: Ashgate, 2006.

[35] E. Hollnagel, The ETTO Principle: Why things that go right sometimes go wrong, Farnham: Ashgate, 2009.

[36] N. Dahlstrom and S. Dekker, "Security and Safety Synergy - Advancing Security With Human Factors Knowledge," in Wiley Handbook of Science and Technology for Homeland Security, John Wiley & Sons, Inc, 2008, pp. 1-13.

[37] D. G. Firesmith, "Common Concepts Underlying Safety, Security and Survivability Engineering, Technical Note CMU/SEI-2003-TN-033," Department of Defense, US, 2003.

[38] A. Burns, J. McDermid and J. Dobson, "On the Meaning of Safety and Security," The Computer Journal, vol. 35, no. 1, pp. 3-15, 1992.

[39] P.-C. Ludovic and C. Claude, "Disentangling the Relations Between Safety and Security," in 9th WSEAS International Conference on Applied Informatics and Communications, Moscow, 2009.

[40] N. Karanikas, "Human Factors Science and Safety Engineering. Can the STAMP Model Serve in Establishing a Common Language?," in Proceedings of the 32nd EAAP Conference, 26-30 September 2016, Cascais, 2017.

[41] B. Holt and D. Fisher, "Managing a Complex Aircraft Systems Investigation," in ISASI Annual Seminar, 22-24 August 2017, San Diego, 2017.

[42] M. Rausand, Risk Assessment: Theory, Methods and Applications, New Jersey: Willey & Sons, 2011.

[43] A. Abdulkhaleq and S. Wagner, XSTAMPP: An eXtensible STAMP Platform As Tool Support for Safety Engineering, Cambridge, MA: Massachusetts Institute of Technology, 2015.

[44] M. Rejzek and S. S. Krauss, STPA Based Hazard and Risk Analysis Tool SAHRA, Cambridge, MA: Massachusetts Institute of Technology, 2017.

[45] M. Rejzek and S. H. Björnsdóttir, Enhanced Risk Management Framework ERMF, Cambridge, MA: Massachusetts Institute of Technology, 2017.