Civil Engineering Research Journal
ISSN: 2575-8950

Juniper PUBLISHERS key to the Researchers

Review Article
Volume 4 Issue 3 - March 2018
DOI: 10.19080/CERJ.2018.04.555640

Civil Eng Res J

Organizational Safety Risk Analysis in Aviation Industry; An STP a Based Framework

Dehghan Nejad A*

Faculty of Health, Safety and Environment, Shahid Beheshti University of Medical Science, Iran

Submission: January 09, 2018; **Published:** April 26, 2018

***Corresponding author:** Ahmad Dehghan Nejad, Faculty of Health, Safety and Environment, Department of Safety Engineering, Shahid Beheshti University of Medical, Science (SBMU), Tehran, Iran, Email: dehghan.nejad@sbmu.ac.ir

Abstract

ICAO recent manuals for both State Safety Policy (SSP) and Safety Management System (SMS) explicitly concentrate on the organizational roots of accidents. The Safety Risk Management (SRM) system, as the core component of both SSP and SMS, consequently are expected to manage the organizational safety risk. In view of that, this paper present a new risk analysis framework that can be feasible to apply as the analyzing logic of the formal SRM; especially, in the start line of the risk management process. For this reason, the framework is founded on the System Theoretic Process Analysis (STPA) to cope with the sociotechnical feature of aviation organization. To apply STPA as the base of the framework, a customized "Feedback Control Loop" is applied to model organizational control mechanisms and extracts their hidden hazards. Furthermore, an innovative concept and procedure are introduced for "Hazard Activation Likelihood" estimation and "HazardConsequences"analysis.

Keywords: STPA; STAMP; SMS; Safety risk analysis; Aviation safety

Abbreviations: SSP: State Safety Policy; SMS: Safety Management System; SRM: Safety Risk Management; STPA: System Theoretic Process Analysis; QC: Quality Control; R&T: Research & Technology HACS: Activation Consequence Severity; HAL: Hazard Activation Likelihood; OSCSC: Organizational Safety Control Structure's Competency

Introduction

Based on Annex 19 of Convention on International Civil Aviation,each State shall establish an SSP for the management of safety in the State, in order to achieve an acceptablelevel of safety performance in civil aviation [1]. Each State also shall require all service providers to implement and maintain an SMS [1]. Since, Safety Risk Management is an important component of both SSP and SMS, not only States but also all aviation service providers must implement an appropriate safety risk management system to support their decision making process.Clearly, the aim of the SMS (and SSP) Safety Risk Managementprocess is to identify and handle all significant influences that may impact on aviation safety, when determining contributing factors for the analysis of consequences of a hazard and deciding on risk mitigation measures.

On the other hand, the pivotal concept of SMS and,consequently, Safety Risk Management systemof wich is concentration on organizational roots of safety hazards and accidents. In fact, in contrast to conventional safety approach,which centers on the technical aspect of the system, the SMS changesthe focus to organizational aspects. This focus changing, of course, is appropriate because many studies have proven that management short comings and organizational aspects are major factors in the occurrence of accidents in complex systems such as aviation industry [2-4].

Based on SMS main concept, which roots in epidemiological accident models, accident's initiating mechanisms do not derive from technical components; rather, originate in organisational and cultural mechanisms, especially the decision-making processes. All aviation service providers thus must tackle these issues throughan appropriate Risk Management system that is equipped with proper techniques to grasp and handle this kind of safety risks.

The main problem is that the safety risks of aviation organizations - as complex and sociotechnical systems-are not extractable only by Conventional Risk Analysis Models (like FMEA, FTA, and other reliability based approaches); especially their complex organizational-based risks. In fact, traditional safety analysis tools, which developed based on pure technical system [5] , are not able to cope with the complexity of sociotechnical systems. Aviation organization thus should apply systemic approach, as recommended by ICAO Doc. 9859, to address their safety issues.

[1]- International Civil Aviation Organization

According to the above, the main objective of this paper isthe proposingof an organizational-based systemic risk analysisapproach, as the central part of the Risk Management System, for preparing an appropriate framework to initiate Safety Risk Management process in aviation organizations.

Accordingly, a clear procedure for organizational hazards identification, as well as a clear logic for hazard probability/ severity analysis is presented in this paper by the following order: at first, the main concepts of Safety Risk Management are reviewed. Then, the principles of STAMP and STPA (as the base models for the presented framework) are expressed. After that, our specific organizational risk analysis framework is described. Afterward, the practicality of the framework is proved by a case study, and finally, the summary and discussion parts are presented.

Main concepts and Based model

Risk management system and the scope of the work

The field of risk management is faced with difficulties in defining and agreeing on principles. Risks are dealt with differently across different countries, industries, and sectors [6]. Although terms, definitions, and interpretations are as varied as the number of sources providing them, we stand our work based on this definition: The Safety Risk Management system is the overall integrated process consisting of two essential interrelated and overlapping, but conceptually distinct components - Risk Assessment and Risk Management[1] [6].

Mullai summarize the fundamental parts of this definition as following [6]:

“Risk assessment” combines both Risk Analysis and Risk Evaluation, providing practically useful and logically structured inputs and perspectives about risks for “Risk Management” (the decision- making process, development of policies, strategies, and measures).

“Risk analysis” is a scientific process in which, by applying a wide range of methods, techniques and tools, risks are identified, estimated, and presented in qualitative and/or quantitative terms. “Risk evaluation” is the process of comparing estimated risks with established risk evaluation criteria (e.g. criteria based on the best available technology, legal requirements, practices, processes, or achievements) in order to determine the level or significance of risks and provide recommendations for the decision-makers at various levels.

Based on the main purpose of this paper, our work is limited to “Risk Analysis” part of risk management system, which includes Hazard Identification and Risk Estimation. The “Risk Estimation” component itself comprises Likelihood Estimation, Consequent Analysis, and Risk Presentation (Present estimated risks based on a specific format such as number, index, color, etc.)

Based model for organizational-based hazard identification

Traditional models of hazard identification, which are summarized as Chain-of-failure-event models, have major inability to handle organizational factors, managerial (social and cultural) roots, and the systemic causes in sociotechnical accidents [7]. In contrast, Systemic approach to technical and organizational safety - which developed by group of researchers, including Rasmussen, Woods, Dekker, Leveson, and Hollnagel, most of whom come from system engineering and human factors backgrounds - is able to appropriately tackle the safety issues of the complex sociotechnical systems [2,8].

The systemic view of safety, and its related techniques, considers accident as the consequence of Hierarchical Safety Control Structures deficiency; therefore, tries to analyze the root cause of gradual deficiencies among the hierarchical control structures by applying holistic and systemic approaches [9]. Related studies have shown that the systemic approaches could be effective tools to model organizational interaction and analyze accident causation within system’s hierarchical control structures [10].

While several researchers have proposed the systems approaches to safety, Leveson’s STAMP (Systems-Theoretic Accident Modeling and Processes) approach has an outstanding superiority and provides a perfect view of the organizational aspects of safety [11].

Systems-theoretic accident modellingand processes (STAMP): STAMP was created to capture more types of accident causal factors including social and organizational structures, new kinds of human error, design and requirements flaws, and dysfunctional interactions among non-failed components. Rather than treating safety as a failure problem or simplifying accidents to a linear chain of events, STAMP treats safety as a hierarchical control problem in which accidents arise from complex dynamic processes that may operate concurrently and interact to create unsafe situations [12].

STAMP taking into account all facets relating the social to the technical aspects, and like the general systems approach to engineering, focuses on the system as a whole, not on the parts or components individually. It assumes that some properties of

[1]- Clearly, Risk Management Process and Risk Analysis- as the process’s core component- are continuous processes that start from preliminary methods to customized, technical, deep, and detailed techniques. While there are a plenty of technical and deep analysis techniques, this paper presented a simple and preliminary – but scientific based- framework for initiating this fundamental process.

[2]In recent years,however, risk communication has become an important integrated component of the Safety Risk Management system. But this component is beyond our work scope.

How to cite this article: Dehghan Nejad A. Organizational Safety Risk Analysis in Aviation Industry; An STP a Based Framework. Civil Eng Res J. 2018; 4(3): 555640. DOI: 10.19080/CERJ.2018.04.555640

systems can be treated adequately only in their entirety. These "system properties" derive from the relationships between parts of systems: how the parts interact and fit together. Concentrating on the analysis and design of the whole as distinct from the components or parts provides an important advantage for STAMP to study safety of the complex systems.

STAMP considers systems as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control [13]. According to this model, accident (systemic accident) could be the result of the dysfunctional performance of adaptation feedback control loop; the controls that may be managerial, organizational, physical, operational, or manufactural. In this view, accidents can be characterized as the resulting from an adaptive feedback function that fails to maintain safety, when performance changes over time to meet a complex and changing set of goals and values [7].

STAMP practicality has been demonstrated by applying it to a number of real and complex systems, including a risk analysis of the organizational structure of the Space Shuttle program after the Columbia loss [14]; tradeoffs among safety, budget, schedule, and performance risks in the new NASA space exploration mission organization [9]; unmanned spacecraft design [15]; a safety assessment of the new U.S. missile defense system; safety in the pharmaceutical industry; and safety of out-patient surgery at Boston's Beth Israel Deaconess Hospital [16], and many other recent studies.

System theoretic process analysis (STPA): Leveson restated that STAMP considers a set of new causality factors for accidents that none of former risk analysis methods can analyze them [13]. She, consequently, developed the STPA method in order to be possible to consider all accident's important aspects and features in process of hazard analysis. Experiences indicate that Leveson has gone the right way because it is admitted by researchers that STPA is significantly more powerful than failure-based techniques in the ability to capture a wider array of hazardous behaviors, including organizational aspects, requirements flaws, design errors, complex human behavior, and component failures. [17]

In respect to STAMP logic, STPA considers accident as result of inadequate control. In fact, STPA accepts that a set of control components and particular interactions have evolved or embedded in system as safety hierarchical control structure; these components and their interrelation mechanisms - in the form of feedback control loop - continually monitor and constrain, by use of Control Actions, the system's behavior to control its dynamicity. In this described condition, accidents occur if a specific control mechanism for restriction of a particular system hazardous behavior doesn't exist or existing control mechanism doesn't able to enforce an expected Control Action.

Basically, STPA concentrates on high-level risks and system's safety constraints to:

- Perform responsibility gap analysis by assessing control components responsibilities and analyzing the probable gap;
- Cognize systemic hazardous behaviors by identifying unsafe Control Actions;
- Accommodate high-level safety constraints into lower levels to control hazardous behaviors; and propose new control mechanisms for enforcement of the new constraints if needed.
- Identify root causes of system's hazardous behavior by analyzing the components of Feedback Control Loop to correct the loops' mechanism.

Although STPA is relatively new compared to traditional methods, it has been demonstrated successfully on a wide range of systems including aviation [18] , spacecraft [19], missile defense systems [20], aviation maintenance [21], civil infrastructure [22], and others.

Additionally, while STPA is a hazard analysis technique developed for analysis and design of system safety architectures, its basis in control theory and system engineering lends to the application of it to social, and non-safety related control and early risk management. Some of the most important samples of this extension include cyber security [23] , business systems and financial operations [24], and the impact of political systems on failures of public infrastructure [25].

The New Approach for Organizational-based Safety Risk Analysis

Why not the original form of STPA

Although the presented risk analysis framework mainly stands on the principles of STPA, this method is not applicable to initiate a formal risk management process in aviation organizations in its original form. This is firstly because the hazard identification process of STPA is fairly complex, detailed and comprehensive. Therefore, it is not appropriate for initiating a formal risk analysis process.

Secondly, and the most important, for the lack of "Risk Estimation Procedure" organizations are not able to use STPA as their formal Risk Analysis Framework; particularly at the initiating phase. In fact, although the STPA - and other STAMP-based methods -have been had invaluable achievement regarding revealing the hidden causes of the catastrophic accident in the complex sociotechnical system, they do not propose a procedure to estimate the risk of the identified hazards. These model, therefore, are not applicable as a formal risk analysis framework [26].

Certainly, the reluctance toward developing a risk estimation procedure - exactly quantification of probability and severity - in STAMP-based methods derives from both essence of the complex systems and the superior awareness of the models'

How to cite this article: Dehghan Nejad A. Organizational Safety Risk Analysis in Aviation Industry; An STP a Based Framework. Civil Eng Res J. 2018; 4(3): 555640. DOI: 10.19080/CERJ.2018.04.555640

architects toward the effect of the system complexity on cause-effect modeling. In fact, while modeling the cause and effect chains between initiating mechanism and the final consequence is the prerequisite step of risk quantification, anticipating and modeling the interrelation between system's components as well as the relation between system behavior (as a consequence) and its components performance is impossible in the complex sociotechnical system. In truth, after finding a specific hazardous performance of a system component, it is impossible to trace all chains of events that may start from that specific hazardous performance and be over to a probable accident scenario. As a result, the probability estimation is impossible. On the other hand, since the specific consequence of the hazardous system's component performance is not clear, the severity of associated consequence is not estimable too.

Nevertheless, if there were enough historical data for making a relation between the "presence of specific hazards" and "occurrence of a particular mishap", the risk estimation would be applicable, even without modeling the cause-effect relations. Enough pertinent data, however, is not available in such complex systems, especially for organizational malfunction mechanisms.

Some researchers have proven that there is very little scientific data validating probabilistic risk assessment or evaluating the methods for calculating it, particularly for complex engineered systems [7, 27,28]. Accordingly, there have been some studies comparing probabilistic risk assessments performed by different groups on the same system where the results indicated large differences in the frequencies calculated for the event [27,29]. In this regard, Leveson mentioned that many major, well-known accidents have occurred in systems where the probability of an accident was previously calculated to be 10^{-9} or less, including Chernobyl, Fukushima, Texas City, Deep Water Horizon, the Therac-25, Challenger, and Columbia, to name but a few [7]. Follensbeealso cites five large transport aircraft accidents and one near accident where the calculated probabilities were 10-9 or less.

Still, Leveson is making a new innovative solution to overcome the problem of "likelihood" in her remarkable hazard analysis approach. Her solution is based on the "Leading Indicators" that can be identified based on the assumptions underlying safety engineering practices and on the vulnerability of those assumptions rather than on likelihood of loss events. In fact, Instead of trying to predict the likelihood that an event will occur or an assumption will fail, the similar but different concept of vulnerability can be used. Vulnerability in the world of assumption-based planning involves assessing whether an assumption could plausibly fail during the lifetime of the system, not the specific probability of that happening [7].

The difference is that instead of trying to assign a numerical likelihood estimate or one of a set of poorly defined categories, only two categories, possible and impossible, are used. That is, if the likelihood is not zero, then the assumption needs to be considered for inclusion in the leading indicators program.

Despite the solution that is being developed by Leveson, we still need a clear "Risk Estimation Procedure" to make it feasible to apply STPA, and its superior hazard identification logic, for organizational risk analysis; even if the estimated risk aren't mathematically meaningful and accurate. In fact, when we focus on Organizational Dysfunctional Mechanisms as the hazards, the exact estimation of failure probability is good-for-nothing. In contrast, we just need a clear Prioritizing Logic to lead the corrective action plan in its right way. So we believe that a proper Risk Estimation Procedure can still be combined with STPA without trapping us on probability estimation obstacles and problems.

Accordingly, a desirable STPA-based organizational risk analysis frameworkfor aviation safety management, which be able to extract the target hazards and prioritize the corrective actions, mustbe made of following parts:

- A framework to model the system's organizational safety control loops (As the initial step of the Hazard Identification Process)
- A clear procedure to extract significant organizational hazards (As the main step of the Hazard Identification Process)
- A framework to estimate Likelihood and Consequence of the hazards; and
- A proper guideline for advanced analysis

In the following, these necessary parts are described to make a partially simple and clear framework for an STPA-based organizational risk analysis procedure.

Hazard Identification

Safety control loops; the roots of the hazards: Based on the STAMP and STPA main concept, accidents occur if Safety Control Structure, which made of a series of inter-connected feedback control loops, cannot be able to control the system behavior. In fact, the feedback control loops deficiency is the main cause of system's uncontrolled behaviors. As the important result, Safety Feedback Control Loops are the "source" of the hazards.

When we add SMS pivotal concepts to the previous argument, the Deficient Safety-Related Organizational Mechanisms are the hidden hazards that we should extract them to control the system's risk. As the bottom line, when we run the STPA-based organizational risk analysis procedure, we should focus on safety-related organizational mechanisms' deficiencies, which are active among Safety Feedback Control Loops, in the hazard identification step.

In the following, the concept of Feedback Control Loop, as the source of hazards, is reviewed.

How to cite this article: Dehghan Nejad A. Organizational Safety Risk Analysis in Aviation Industry; An STP a Based Framework. Civil Eng Res J. 2018; 4(3): 555640. DOI: 10.19080/CERJ.2018.04.555640

Feedback control loop and process model: Based on the control theory, the four following conditions are required inorder to control a processby a control component [13]:

- Goal Condition: The controller must have a goal or goals.
- Action Condition (or controllability condition): The controller must be able to affect the state of the system. In engineering, Control Actions are implemented by actuators.
- Model Condition: The controller must be (or contain) a model of the system.
- Observability Condition: The controller must be able to as certain the state of the system. In engineering terminology, observation of the state of the system is provided by sensors.

These conditions are the requirements of the fundamental loop in the control theory that have been named as "Feedback Control Loop". In control theory, open systems are viewed asinterrelated components that are kept in a state of dynamic equilibrium by feedback loops of information (communication) and control mechanisms. These loops also have a paramount position in STAMP and STPA method, as the models that were based on the control theory, because STAMP and STPA consider accidents as the control problems.

Figure 1 displays a typical technical control loop for controlling information about (observes) the process state from measured variables (feedback) and uses this information to initiate action by manipulating controlled variables to keep the process operating with inpredefined limits or setpoints (the goal) despite disturbances to the process.

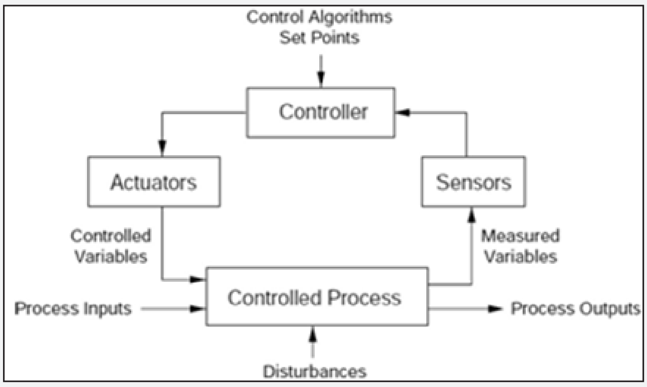


Figure 1: A standard control loop [13].

In this loop, Process Models have a significant role, because automate (or human) controllers must be able to simulate the under controlled process in their logic (or mind) for enforcement of Control Action to keep the process operation within predefined limits. Every controller, in fact, must contain a model of the processes that are being controlled. Accidents happen when the controller's Process Model does not match the system that is being controlled and, consequently, the controller issues inappropriate commands [13]. Figure 2 shows a general control loop and its process model.

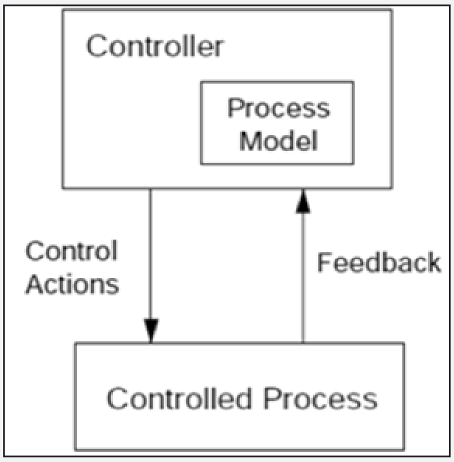


Figure 2: Control loop with process model [13].

Organizational components need the same tools to do their control duties; however, the type of the loop's components and variables may be somewhat different. For example, organizational variables and goals are not as clear as the technical variables. Furthermore, feedback and actuator channels in organizational control loops are forms and formal requests or reports; instead of signals or other technical tools that usually are used in technical loops [21].

Moreover, Control Processes in organizational control loops are not a mathematical function or logical algorithms. Actually, organizational loops' control processes almost are a form of unclear decision-making models that exist in decision makers' mind; the persons who are engaging in decision making in the different level of the organizational hierarchy. In fact, they may be either a technician, for technical decision-making, or a top or middle manager for strategic or executive decisions.

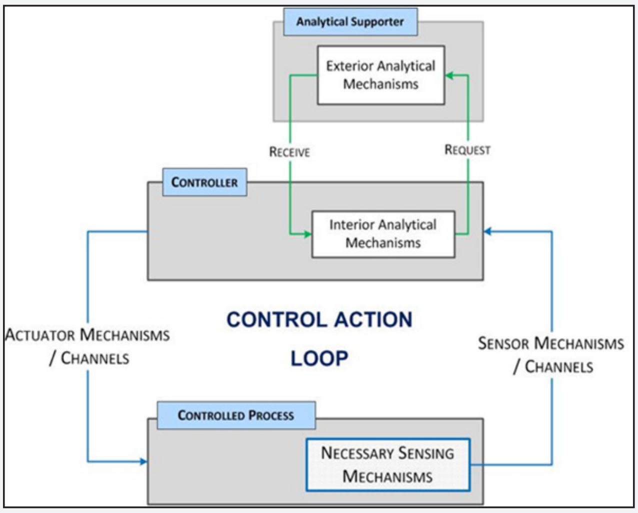

Analytical Supporter
Exterior Analytical Mechanisms
Receive
Request
Controller
Interior Analytical Mechanisms
Actuator Mechanisms / Channels
CONTROL ACTION LOOP
Sensor Mechanisms / Channels
Controlled Process
Necessary Sensing Mechanisms

Figure 3: Specific Organizational Feedback Control Loops together with Customized Process Model [21].

Organizational feedback control loop: In order to apply STPA for initiating organizational hazard analysis, as the main reason of this paper, it is needed to use a specific version of the feedback control loop that was exclusively developed for deficiency analysis of organizational safety control mechanisms. Figure 3 presents thisspecific Organizational Feedback Control Loop to gether with its customized Process Model [21]. Based on Figure 3, five requirements shall be met to accurately enforce the Control Actions by organizational control components:

a. A Necessary Sensing Mechanism must be active in the process under control to collect, process, and prepare accurate information for the control component. This mechanism is a type of organizational processes that may be managed by either main control component of the loop or other organizational components.

b. A reliable Sensor Mechanism (or channels) must be active for delivering the prepared information to the control component. This mechanism is also a type of organizational communication channel.

c. An Analytical Mechanism must be active for accurate processing of received information to determine appropriate Control Action. This mechanism is also a type of organizational processes. While Interior Analytical Mechanism is applied by the control component of the loop, Exterior Analytical Mechanism is applied via other organizational components (in a situation that exterior analyzing is needed).

d. A reliable Request-Receive Mechanism must be active to receive necessary information from other components (in a situation that exterior analyzing is needed). This mechanism also is a type of organizational process, which prepares appropriate context for information exchange between Interior and Exterior Analytical Mechanisms.

e. A reliable Actuator Mechanism (or channels) must be active to enforce the Control Action to under control process. This mechanism is also a type of organizational communication channel.

Modelling the system's organizational safety control loops: Based on Figure 4, for modeling the system organizational safety control loops (As the initial step of the Hazard Identification Process) a sequence of procedures are needed that are described in the following.

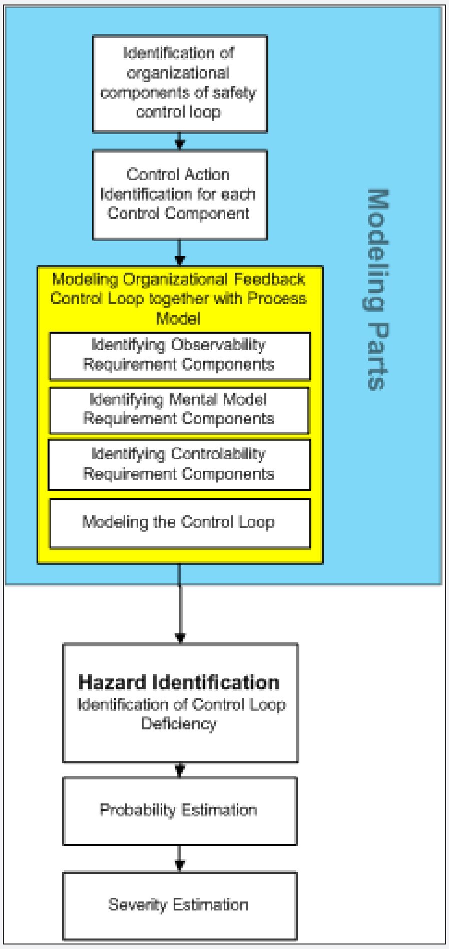

Identification of organizational components of safety control loop
Control Action Identification for each Control Component
Modeling Organizational Feedback Control Loop together with Process Model
Identifying Observability Requirement Components
Identifying Mental Model Requirement Components
Identifying Controlability Requirement Components
Modeling the Control Loop
Modeling Parts
Hazard Identification
Identification of Control Loop Deficiency
Probability Estimation
Severity Estimation

Figure 4 : Main steps of the STPA-based Risk Analysis.

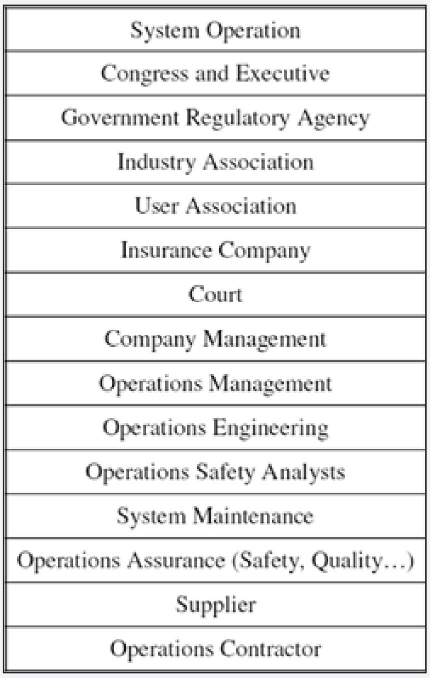
How to cite this article: Dehghan Nejad A. Organizational Safety Risk Analysis in Aviation Industry; An STP a Based Framework. Civil Eng Res J. 2018; 4(3): 555640. DOI: 10.19080/CERJ.2018.04.555640

Identification of organizational components of safetycontrol loop : Before modeling the safety control loops for each control action of all control components, as a main part of STPA, the control components must be identified. Since our risk analysis model concentrates on organizational roots of probable accidents, we focus on "organizational control components" and their associated control actions.

Dulac recommended three important in formation sources to identify Safety control Structure's organizational components. Additionally, he recommended two criteria to summarize this information for elicitation best set of these components [30]. These recommendations are reviewed as follow:

a. **Org charts (Source one):** He mentioned that, organization's charts are a good start line for identification of organizational components.

b. **Generic STAMP structures (Source two):** The generic control structure that was shown in Figure 5, can be used as an effective checklist to verify that important components have not been mistakenly left out. He noted that, for many systems, it is unneeded to follow the hierarchical structure all the way up to the Congress and Executive components.

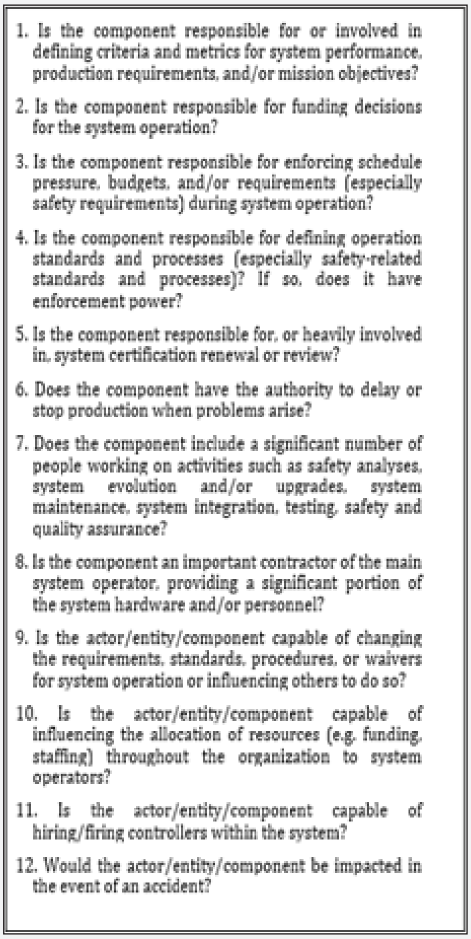


System Operation
Congress and Executive
Government Regulatory Agency
Industry Association
User Association
Insurance Company
Court
Company Management
Operations Management
Operations Engineering
Operations Safety Analysts
System Maintenance
Operations Assurance (Safety, Quality…)
Supplier
Operations Contractor

Figure 5 : The generic control structure [13].

c. **Interview data (Source 3):** Another source for identification safety control structure's organizational components is the interviewing from individuals within the structure itself. Dulac stated that the emphasis should be on reviewing, improving and refining the structure, eliciting informal structural connections that are not represented in the official ''party-line'' organization chart.

d. **Inclusion criteria (Criterion 1):** He prepared eight questions in order to decide whether an organization component should be included in the model or not. However, Stringfellow has added four more questions to the list for consideration of more social features of the control structure [31]. Figure 6 lists the complete questions.



1. Is the component responsible for or involved in defining criteria and metrics for system performance, production requirements, and/or mission objectives?
2. Is the component responsible for funding decisions for the system operation?
3. Is the component responsible for enforcing schedule pressure, budgets, and/or requirements (especially safety requirements) during system operation?
4. Is the component responsible for defining operation standards and processes (especially safety-related standards and processes)? If so, does it have enforcement power?
5. Is the component responsible for, or heavily involved in, system certification renewal or review?
6. Does the component have the authority to delay or stop production when problems arise?
7. Does the component include a significant number of people working on activities such as safety analyses, system evolution and/or upgrades, system maintenance, system integration, testing, safety and quality assurance?
8. Is the component an important contractor of the main system operator, providing a significant portion of the system hardware and/or personnel?
9. Is the actor/entity/component capable of changing the requirements, standards, procedures, or waivers for system operation or influencing others to do so?
10. Is the actor/entity/component capable of influencing the allocation of resources (e.g. funding, staffing) throughout the organization to system operators?
11. Is the actor/entity/component capable of hiring/firing controllers within the system?
12. Would the actor/entity/component be impacted in the event of an accident?

Figure6 : List of development and operation generic components [30].

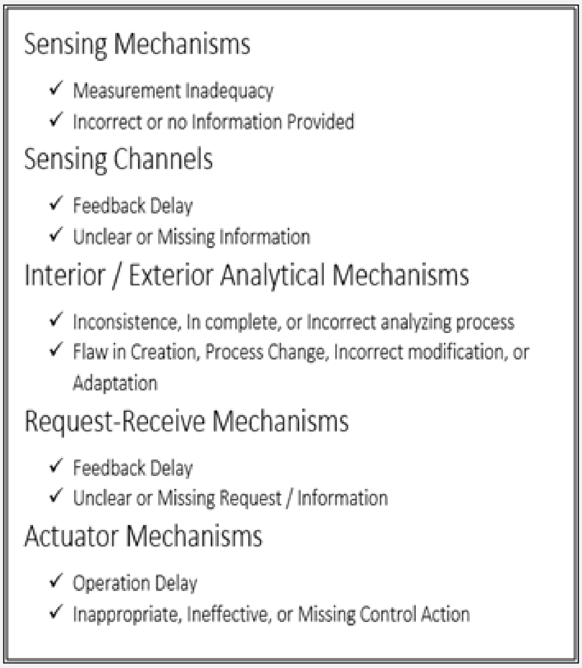
e. **Combination criteria (Criterion 2):** For preventing of unnecessary complexity in control structure's model, it can be possible and desirable to combine multiple components. As a general rule, components that are structurally independent, but functionally similar, should be combined unless they receive funding from completely different or competing sources, or if they have competing.

Control actions identification: Control Actions are the actions that are enforced by control components to control the system behaviors. Clearly, Control Actions are the reason d'etre of the control components.It should be noted that, each identified control components may apply different Control Actions to control their under control processes; therefore, identifying all components' Control Actions just is possible by scrutinizing all of related documents and interviewing with organizational experts. Finally, the results should be listed in an appropriate log [32].

Organizational feedback control loop modelling: Now, in order to model organizational Feedback Control Loops - based on the mentioned exclusive modelling diagram - all Non-Control Actions (Necessary Sensing Mechanisms and Analytical Mechanisms) must be explored for each control component. Then, all requisite mechanisms, as the Non-Control Actions, for accurate enforcement of each Control Action must be specified. Finally, all Feedback Control Loops - together with their Process Model - must be modeled according to the pattern that has been presented in Figure 3.

Organizational hazard identification: ''Working around the loop'' is the STPA's principle to extract the hazards. In fact, each of control loop's component should be regarded as a potential source of systemic hazard; because any inefficient performance of them can be able to cause a degree of incompetency in the control loop. This local deficiency, consequently, eventuate to a level of inefficiency in the whole system safety control structure; and, in a bigger picture, leads to the system accost to a probable accident [33].

Accordingly, by using the Simplified General Causal Factors, which are adapted from STPA original model and shown in Figure 7, different statuses of "Control Component Inefficiency" could be extracted and regarded as the initiating mechanisms for systemic accidents. These initiating mechanisms thus should be recorded as a specific hazard for the probability and consequence estimation.



Sensing Mechanisms

- ✓ Measurement Inadequacy
- ✓ Incorrect or no Information Provided

Sensing Channels

- ✓ Feedback Delay
- ✓ Unclear or Missing Information

Interior / Exterior Analytical Mechanisms

- ✓ Inconsistence, In complete, or Incorrect analyzing process
- ✓ Flaw in Creation, Process Change, Incorrect modification, or Adaptation

Request-Receive Mechanisms

- ✓ Feedback Delay
- ✓ Unclear or Missing Request / Information

Actuator Mechanisms

- ✓ Operation Delay
- ✓ Inappropriate, Ineffective, or Missing Control Action

Figure 7 : Simplified Causal Factors for Control Loop Deficiency.

Risk estimation

Hazard activation likelihood (HAL): While hazard is a dangerous dormant situation that triggers a mishap if will be activated, the likelihood of the hazard is the probability of the hazard activation. When we consider the hazard as the Deficiency in organizational safety control mechanisms, we prepare this opportunity to evaluate the Hazard Activation Likelihood (HAL) via the ratio of the imperfect performances of the mechanism and the desired performance of it at a specific period. Also, we can make a qualitative conception of HAL by regarding experts' opinions and applying Table 1, if the reliable performance data is not available [34].

Table 1: Hazard Activation Likelihood (HAL) Estimation Table.

Likelihood	Meaning	Value
Frequent	The deficiency likely to occur many time (has occurred frequently)	5
Occasion	The deficiency likely to occur sometimes (has occurred frequently)	4
Remote	The deficiency unlikely to occur, but possible (has occurred rarely)	3
Improbable	The deficiency very unlikely to occur (not known to have occurred)	2
Extremely Improbable	Almost inconceivable that the deficient performance will occur	1

Hazard activation consequences severity (HACS) analysis: In addition to Hazard Activation Likelihood estimation, we need a clear rule to estimate the Hazard Activation Consequences Severity (HACS), if we want to estimate the risk of any hazards.

For making an appropriate way to estimate the severity of the hazard activation consequences, we change the concept of "consequence" from the real results of hazard activation (happening the real mishap) to a new measurable quality that directly linked to control theory. Actually, instead of seeking and modeling the imperceptible results of defective mechanisms (as the hazards) on the probable accident scenarios, we focus on the negative consequence of the identified defective mechanisms on the whole Organizational Safety Control Structure's Competency (OSCSC).

This substitution can be meaningful because based on STAMP pivotal thought, accidents in complex sociotechnical system happen when the safety control structure cannot be able to control the system's behavior. As a result, it can be hypothesized that a defective mechanisms are able to cause a kind of deterioration on the safety control structure, and then, the dormant systemic hazards become active and initiate a complex and imperceptible chain of events that finally eventuate to a mishap; or at least, can push the system toward a more hazardous situation [35].

When it is impossible to estimate the role of a specific defective mechanism on the formation of accident scenarios, it can be feasible to be focused on "consequent deterioration" in safety control structure; the deterioration that can be regarded as a preceding status of a probable catastrophic accident.

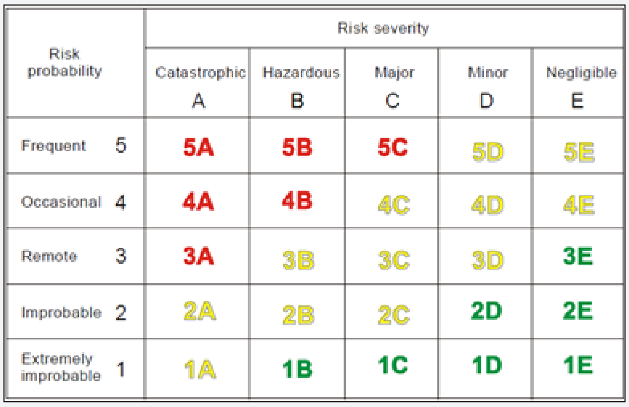
The whole OSCSC is an abstract concept that shows "how well safety control structure enforces desirable system safety constraints". This concept stands on the system theory, the control theory, and specifically, main concept of STAMP and STPA model. According to these theories and models, the main mission of "Safety Control Structure" is to enforce specific constraints to ensure that the system will be keeping in a safe zone when has to tolerate unavoidable and continuous changes. In fact, system's control structure must have an appropriate dynamicity to constrain the real dynamic system in each new position.Nevertheless, in a specific point of time, the real control structure may not completely conform to the desired control structure. This unconformity and gap may have some causes such as control structure design inappropriacy, imperfective performances of some control structure's components, or unfit adaptation of the control structure [36].

Accordingly, the whole OSCSC is a concept that can be able to reflect the experts' overall opinion about the real control structure proficiency. The experts, in fact, are able to qualitatively estimate the effect of a specific deficient mechanism, which was explored in the hazard identification phase, on the Safety Control Structure's Competency. The severity of this effect, consequently, is able to take the place of the "Hazard Severity" in the risk analysis procedure [37].

Risk evaluation

Risk evaluation is the process of comparing estimated risks with established risk evaluation

Case Study (Figure 8-10)



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

Figure 8 : Risk Evaluation Table [1].

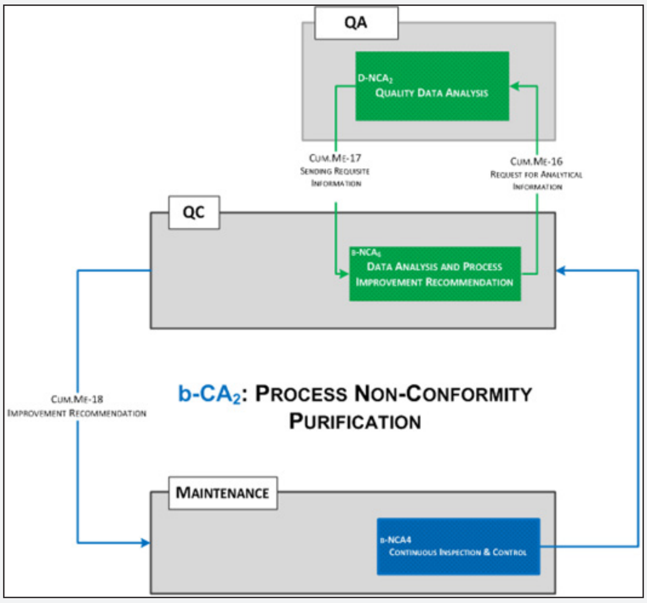

QA
D-NCA$_2$
Quality Data Analysis
Cum.Me-17
Sending Requisite Information
Cum.Me-16
Request for Analytical Information
QC
b-NCA$_4$
Data Analysis and Process Improvement Recommendation
Cum.Me-18
Improvement Recommendation
b-CA$_2$: Process Non-Conformity Purification
Maintenance
b-NCA4
Continuous Inspection & Control

Figure 9 : The feedback control loop for Quality Control (QC) unit.

How to cite this article: Dehghan Nejad A. Organizational Safety Risk Analysis in Aviation Industry; An STP a Based Framework. Civil Eng Res J. 2018; 4(3): 555640. DOI: 10.19080/CERJ.2018.04.555640

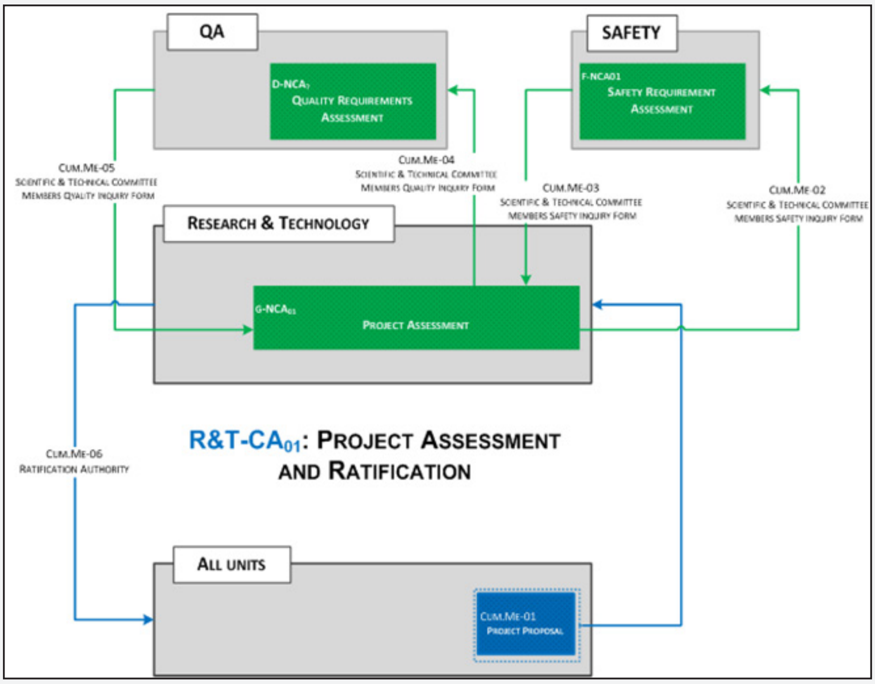
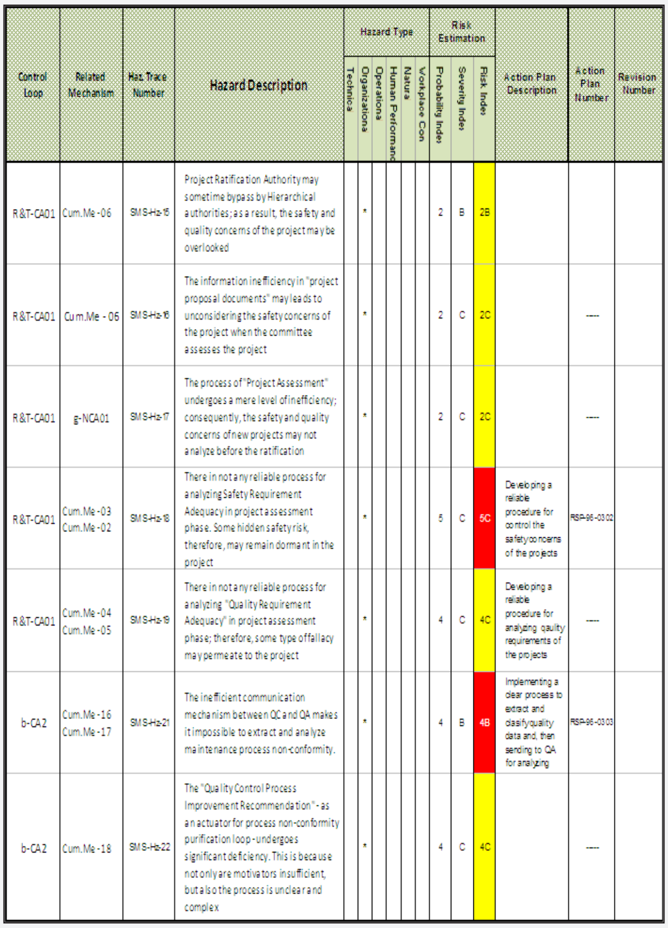

QA
D-NCA7
Quality Requirements Assessment
Safety
F-NCA01
Safety Requirement Assessment
Cum.Me-05
Scientific & Technical Committee Members Quality Inquiry Form
Cum.Me-04
Scientific & Technical Committee Members Quality Inquiry Form
Cum.Me-03
Scientific & Technical Committee Members Safety Inquiry Form
Cum.Me-02
Scientific & Technical Committee Members Safety Inquiry Form
Research & Technology
G-NCA01
Project Assessment
Cum.Me-06
Ratification Authority
R&T-CA01: Project Assessment and Ratification
All units
Cum.Me-01
Project Proposal

Figure 10 : The feedback control loop for R&T unit.

Summary and Results (Figure 11)



Control Loop	Related Mechanism	Haz. Trace Number	Hazard Description	Hazard Type						Risk Estimation			Action Plan Description	Action Plan Number	Revision Number
				Technica	Organizationa	Operationa	Human Performanc	Natura	Workplace Con	Probability Index	Severity Index	Risk Index			
R&T-CA01	Cum.Me-06	SMS-Hz-15	Project Ratification Authority may sometime bypass by Hierarchical authorities; as a result, the safety and quality concerns of the project may be overlooked		*					2	B	2B			
R&T-CA01	Cum.Me - 06	SMS-Hz-16	The information inefficiency in "project proposal documents" may leads to unconsidering the safety concerns of the project when the committee assesses the project		*					2	C	2C		----	
R&T-CA01	g-NCA01	SMS-Hz-17	The process of "Project Assessment" undergoes a mere level of inefficiency; consequently, the safety and quality concerns of new projects may not analyze before the ratification		*					2	C	2C		----	
R&T-CA01	Cum.Me-03 Cum.Me-02	SMS-Hz-18	There in not any reliable process for analyzing Safety Requirement Adequacy in project assessment phase. Some hidden safety risk, therefore, may remain dormant in the project		*					5	C	5C	Developing a reliable procedure for control the safety concerns of the projects	RSP-96-0302	
R&T-CA01	Cum.Me-04 Cum.Me-05	SMS-Hz-19	There in not any reliable process for analyzing "Quality Requirement Adequacy" in project assessment phase; therefore, some type of fallacy may permeate to the project		*					4	C	4C	Developing a reliable procedure for analyzing qaulity requirements of the projects	----	
b-CA2	Cum.Me-16 Cum.Me-17	SMS-Hz-21	The inefficient communication mechanism between QC and QA makes it impossible to extract and analyze maintenance process non-conformity.		*					4	B	4B	Implementing a clear process to extract and clasify quality data and, then sending to QA for analyzing	RSP-96-0303	
b-CA2	Cum.Me-18	SMS-Hz-22	The "Quality Control Process Improvement Recommendation" - as an actuator for process non-conformity purification loop - undergoes significant deficiency. This is because not only are motivators insufficient, but also the process is unclear and complex		*					4	C	4C		----	

Figure 11 : Risk Analysis Results for QC and R&T.

Conclusion and Discussion

For precise evaluation of OSCSC, certainly, we need more data to model the relation network between safety structure's components;nevertheless, in the initiating phase of organizational risk analysis we can rely on experts judgment.

Table 2 is presented to estimates the severity of a consequence that is initiated from specific organizational hazard by extracting experts' opinions.

Table 2: Hazard Activation Consequence Severity (HACS) Estimation Table.

Severity	Meaning	Value
Catastrophic	Completely Terminate the Safety Control Structure Consistency	A
Hazardous	Cause a Large Reduction in Safety Control Structure Consistency	B
Major	Cause a Significant Reduction in Safety Control Structure Consistency	C
Minor	Cause a Nuisance Reduction in Safety Control Structure Consistency	D
Negligible	Cause a Few Reduction in Safety Control Structure Consistency	E

Finally, the estimated risk is described in a qualitative term by a combination of two characters that the first demonstrates the Hazard Activation Likelihood (HAL) and the second demonstrates the Hazard Activation Consequence Severity (HACS); such as 3A, 5B and the like.

Criteria (e.g. criteria based on the best available technology, legal requirements, practices, processes, or achievements) in order to determine the level or significance of risks and provide recommendations for the decision-makers at various levels [6]. Although "Risk Evaluation" is beyond this paper's scope, 'As Low As Reasonably Practicable' (ALARP) strategy usually employs for managing the risks. In the case study section, a simple table is applied as a sample for the risk evaluation criteria.

In the following, the presented STPA-based organizational risk analysis framework is applied - in limited scale - to extract organizational safety-related hazards and estimate their risk. The case is a sample aviation industry that is responsible for maintenance and modification of Iran's helicopter fleet.

Accordingly, only two organizational safety control components together with their related communication mechanisms, and their inter-connected non-control components (analyzing or supporting components) were selected for further analysis. These two organizational components include Quality Control (QC) unit, and Research & Technology (R&T) unit. The first one is responsible for managing the main and the most comprehensive control mechanisms in case industry. The second one controls modification projects via its ratification authority.

Based on the modeling pattern, which is illustrated in Figure 3, all control requisite mechanisms have been identified and, then, the control loops have been made (Figure 8 For QC and Figure 9 for R&T).

After modeling the control loops, all parts of the loops have been analyzed by means of the Simplified Causal Factors (Figure 7) in order to extract any probable deficiency; then, a group of experts estimated the probability of each extracted deficiencies via applying Table 1. This group of expert, then, applied Table 2. to estimate the probable consequence of the identified hazards on the whole OSCSC; after all, the risks of the hazards are evaluated by means of Figure 10; as a simple method for prioritizing the necessary control actions. Finally, the results have been summarized and depicted in Figure 11.

For initiating the process of organizational-based safety risk analysis in aviation industries, which is needed concerning ICAO's safety management system (SMS), an innovative and specific framework have been presented in this paper. This framework was built on the Control Theory and, specifically, the STPA model. Based on this model's main concept, catastrophic accidents in complex socio-technical systems originate from the Safety Control Structure deficiency. Accordingly, the new framework is concentrated on Organizational Safety Control Loops deficiency (as the hidden hazards) and the effect of these deficiencies on the whole Organizational Safety Control Structure Competency (as the consequence of the hazards).

For presenting the main procedures of the framework, its modeling and analyzing parts were described separately. The modeling part is made of a series of steps to identify organizational control components, control actions, and model the control loops. The analyzing part is responsible for extracting defective mechanisms that are placed in control loops by use of a series of guide-words, which is named Simplified Causal Factors. This part also is responsible for evaluating the Hazard Activation Likelihood and the severity of Hazard Activation consequences.

For estimating likelihood of the hazards and severity of the consequences, two specific tables were presented as the guide tools for experts' judgment. Finally, the framework was limitedly applied in a case aviation organization to clear its sequence and procedures, as well as its applicability.

The presented framework is developed for analyzing the organizational-based safety hazards that are hidden in the operational phase of the system. We, consequently, assumed that all high-level hazards of the system had been identified and adequate control components with clear responsibilities had been embedded in the system to control them; however, it is possible that some of the control mechanisms had been eroded or outdated in the result of system dynamic behavior.

According to this assumption, we neglected some of initiating steps of STPA that are related to "System-Level Hazard

How to cite this article: Dehghan Nejad A. Organizational Safety Risk Analysis in Aviation Industry; An STP a Based Framework. Civil Eng Res J. 2018; 4(3): 555640. DOI: 10.19080/CERJ.2018.04.555640

Identification" and "Safety Constraints Identification". In fact, we started the hazard identification process from extracting current organizational control components and their responsibilities. Nevertheless, we admit that a comprehensive analysis, which should be done in the next rounds of a continuous risk management cycle, must start at "System-Level Hazard Identification" and continue separately for each system-level hazard.

Furthermore, a more advanced analysis should be developed based on more quantitative and precise data for "Hazard Activation Likelihood" and "Hazard Activation Consequences Severity" estimation. Increasing preciseness of these two quantities can be able to help system engineers and decision-makers to find and concentrate critical mechanisms of the control structure for launching more appropriate improvement plans.

In addition, the evaluated risk (the combination of HAL and HACS) of each safety-related organizational mechanism has a meaningful dynamic feature. This is because both the imperfect ratio of organizational mechanisms and the whole Organizational Safety Control Structure Competency are sensitive to organizational dynamicity. As an important result, the estimated risk could help system engineers to design remarkable leading indicators as the predecessor of system hazardous behaviors.

References

1. Annex ICAO (2013) To the Convention on International Civil Aviation, safety management, first. 19: 1-2.
2. Rasmussen, Jens (1997) Risk management in a dynamic society: a modelling problem. Safety science 27(2): 183-213.
3. Turner, Barry A, Nick F, Pidgeon (1997) Man-made disasters. Vol. 2. Oxford: Butterworth-Heinemann.
4. Reason, James (2016) Managing the risks of organizational accidents. Routledge.
5. Hollnagel E (2010) Understanding accidents-from root causes to performance variability. Human factors and power plants, 2002. Proceedings of the 2002 ieee 7th conference on. IEEE, 2002.
6. Mullai, Arben (2006) Risk management system-risk assessment frameworks and techniques. Vol. 5. No. 2006. DaGoB (Safe and Reliable Transport Chains of Dangerous Goods in the Baltic Sea Region) Project Office, Turku School of Economics, Turku, Finland.
7. Leveson Nancy (2015) A systems approach to risk management through leading safety indicators. Reliability Engineering & System Safety 136: 17-34.
8. Dekker S (2005) Ten Questions about Human Error: A new view of human factors and system safety, CRC Press.
9. Dulac, Nicolas, Brandon D Owens, Nancy G Leveson (2007) Modelling Risk Management in the Development of Space Exploration Systems. Proceedings of the 2nd Annual International Association for the Advancement of Space Safety (IAASS) Conference.
10. Kontogiannis, Tom, Stathis Malakis (2012) Recursive modeling of loss of control in human and organizational processes: A systemic model for accident analysis. Accident Analysis & Prevention 48 (2012): 303-316.
11. Leveson N, Dulac N, Marais K, Carroll J (2009) Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems. Organization studies 30(2-3): 227-249.
12. Chung N (2014) Systems-Theoretic Process Analysis of the Air Force Test Center Safety Management System. Diss. Massachusetts Institute of Technology.
13. Leveson N (2011) Engineering a safer world: Systems thinking applied to safety. MIT press, 2011.
14. Leveson NG (2005) Modelling, Analyzing and Engineering Safety Culture. ESA Special Publication. Vol. 599.
15. Owens BD, Herring MS, Dulac N, Leveson NG (2008) Application of a safety-driven design methodology to an outer planet exploration mission. Aerospace Conference, 2008 IEEE.
16. Dierks, Meghan, Nicolas Dulac, Leveson N, Margaret SF (2008) System dynamics approach to modeling risk in complex healthcare settings. Proceedings of the System Dynamics Conference, Athens Greece.
17. Blake A, Arterburn D, Jon Schneider DH, Brandon A, Leveson N (2016) A New Approach to Hazard Analysis for Rotorcraft. American Helicopter Society Specialists Meeting on Development, Affordability, and Qualification.
18. Fleming CH, Spencer M, Thomas J, Leveson NG, Wilkinson C (2013) Safety assurance in NextGen and complex transportation systems. Safety science 55 (2013): 173-187.
19. Takuto I, Leveson NG, Thomas J, Katahira M, Miyamoto Y, et al. (2010) Modeling and hazard analysis using STPA.
20. Pereira SJ, Grady L, Jeffrey H (2006) A system-theoretic hazard analysis methodology for a non-advocate safety assessment of the ballistic missile defense system. MISSILE DEFENSE AGENCY WASHINGTON DC.
21. Dehghan Nejad A, Gholamnia R, Alibabaee, A (2017) Int J Syst Assur Eng Manag, 8(Suppl 2): 1008.
22. Airong D (2012) Application of CAST and STPA to railroad safety in China. Diss Massachusetts Institute of Technology.
23. Young W, Leveson NG (2014) An Integrated Approach to Safety and Security Based on Systems Theory, Commun. ACM 57(2): 31-35.
24. Buck W (2013) STAMP as a Theoretical Framework for Understanding Corporate Moral Failure: A systems approach to corporate social responsibility, presented at the 2013 STAMP Conference.
25. Abdymomunov (2011) Application of system safety framework in hybrid socio-technical environment of Eurasia.
26. Torbjørn B, Terje A, Enrico Z (2016) Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. Reliability Engineering & System Safety 156: 203-209.
27. Rae A, McDermid J, Rob A (2012) The science and superstition of quantitative risk assessment, Proceedings of Probabilistic Safety Assessment and Management (PSAM) Conference 11, International Association for Probabilistic Safety Assessment and Management (IAPSAM), Helsinki, June 2012, pp. 2292-2301.
28. Manion M (2007) The epistemology of fault tree analysis: An ethical critique. Int. Journal of Risk Assessment and Management, 7(3).
29. Leveson N, Safeware B (1995) Addison-Wesley Publishers.
30. Dulac N (2007) A Framework for dynamic safety and risk management modeling in complex engineering systems. Diss. Massachusetts Institute of Technology.
31. Margaret SFV (2010) Accident analysis and hazard analysis for human and organizational factors. Diss. Massachusetts Institute of Technology.

How to cite this article: Dehghan Nejad A. Organizational Safety Risk Analysis in Aviation Industry; An STP a Based Framework. Civil Eng Res J. 2018; 4(3): 555640. DOI: 10.19080/CERJ.2018.04.555640

32. Nejad DA (2015) Effect analysis of organizational safety control structure on aircraft reliability in maintenance industry. M.Sc. Dissertation, Shahid Beheshti University of Medical Sciences.

33. Doc ICAO (2006) 9859 Safety Management Manual. ICAO. Kanada.

34. Fleming C (2011) Safety guided spacecraft design using model-based specifications. Proceedings of the 5th IAASS Conference.

35. Nakao H, Katahira M, Miyamoto Y, Leveson NG (2011) Safety guided design of crew return vehicle in concept design phase using STAMP/STPA. Proc. of the 5th IAASS Conference.

36. Qureshi Zahid H (2007) A review of accident modelling approaches for complex socio-technical systems. Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems-Volume 86. Australian Computer Society, Inc.

37. Woods DD, Johannesen LJ, Cook RI, Sarter NB (2010) Behind Human Error Ashgate Publishing Company.

DOI: 10.19080/CERJ.2018.04.555640

How to cite this article: Dehghan Nejad A. Organizational Safety Risk Analysis in Aviation Industry; An STP a Based Framework. Civil Eng Res J. 2018; 4(3): 555640. DOI: 10.19080/CERJ.2018.04.555640