SYSTEMS-THEORETIC AND ACCIDENT MODEL AND PROCESSES (STAMP) APPLIED TO DESIGN A SAFETY-DRIVEN CONCEPT OF AN AIR NAVIGATION SERVICE PROVIDER (ANSP)

Bemildo Alvaro Ferreira Filho
Brazilian Air Traffic Controllers' Associations Federation – FEBRACTA
Safety Analysis Group (GAS) - contributor
FVPSudeste@gmail.com

João Batista Camargo Junior
Safety Analysis Group (GAS)
University of São Paulo (Poli-USP)
joao.camargo@poli.usp.br

ABSTRACT

The present study has as its main assumption that the safety-critical organizations prone to experience accidents with loss of lives or investments of great impact on society cannot be treated as any other organization with no such intrinsic characteristic. In general, such organizations are highly automated, have more complex coupled subsystems and also have the tendency to shift workers' duties from active roles to supervisory roles. This paper proposes the use of Systems-Theoretic Accident Models and Processes (STAMP), and its tool Systems-Theoretic Process Analysis (STPA) as a new type of hazard analysis technique, to help designing an air navigation service provider (ANSP) organization ready not only to cope with the demands of the current clearance-based operations (CBO), but with the transition phase to trajectory-based operations (TBO), and with the TBO concept itself as well.

Keywords: Systems theory, STAMP, STPA, safety, ANSP.

1. INTRODUCTION

After the midair collision over the Brazilian rainforest on 29 September 2006 discussions were started among many stakeholders of the Brazilian Civil Aviation System with the sole intent of seeking the causes of the worst accident involving Brazilian air traffic control. Nevertheless we noticed that little time was spent to analyzing the administrative organization of the Brazilian air navigation service provider (ANSP) by the Government meetings with aviation stakeholders, the Brazilian Congress hearings or even the accident investigation Final Report.

This paper proposes the use of Systems-Theoretic Accident Models and Processes (STAMP), and its tool Systems-Theoretic Process Analysis (STPA) as a new type of hazard analysis technique, to help designing an air navigation service provider (ANSP) organization.

The assumption is that system theory, and STAMP as a theoretical foundation for engineering a new safe system, will help ANSP managers to cope with the demands of the current clearance-based operations (CBO), but with the transition phase to trajectory-based operations (TBO), the TBO concept itself and the air traffic forecasts for the next three decades as well.

2. HISTORICAL CONTEXT

2.1. Accidents involving the Brazilian ANSP

The worst air crash directly involving Brazilian air traffic control killed 154 people and occurred in controlled airspace between two aircraft carrying up-to-date technology to support the flights (CENIPA, 2008). One of the flights was a Brazilian Embraer business jet being delivered to a company in the United States of America and the crew was allegedly not familiar with the Brazilian ATC work culture. This aircraft suffered minor damage and all the passengers and crew landed safely at a Brazilian Air Force (FAB) base in the Amazon rainforest. The other one was a jetliner from Boeing flying a regular scheduled flight for a Brazilian airline. This aircraft had one of its wings cut and performed an inevitable dive into the dense jungle.

Twenty years before, on 19 September 1986 (CENIPA, 1986), there was an apparently similar accident concerning ATC procedures, also with a foreign crew delivering a twin turboprop Embraer aircraft to a US company. The aircraft crashed into a mountain a few minutes after its departure and killed both the pilot in command and the first officer plus three passengers.

According to the Final Reports of both losses, the Brazilian air traffic control played a significant operational contribution to these accidents, notably regarding the clearance of the filed flight plan and the English language proficiency of the involved air traffic controllers.

2.2. Civil aviation authorities in Brazil

Two years after the creation of the International Civil Aviation Organization (ICAO) on 7 December 1944, by what is known as the Chicago Convention (ICAO, 1944), the Brazilian Air Force created the embryo of the current Brazilian airspace control organization named DECEA. DECEA stands for Department of Airspace Control and according to its website it is “responsible for the management of all the activities related to the safety and efficiency of Brazilian airspace control. Its mission is to manage and control air traffic in sovereign Brazilian airspace as well as to guarantee its defense” (DECEA, 2014a). DECEA is a branch of the Air Command of the Brazilian Air Force (FAB), a military organization under the Ministry of Defense’s jurisdiction.

The Brazilian Government created in September 2005 a counterpart of DECEA for Brazilian civil aviation by replacing the former military organization known as Civil

Aviation Department (DAC). The National Civil Aviation Agency (ANAC) is the current regulatory body responsible for the regulation and the safety oversight of civil aviation (ANAC, 2014). It covers all aspects of civil aviation regulatory matters except those related to control and defense of Brazilian airspace. ANAC is under jurisdiction of another ministry, the Secretariat of Civil Aviation of the Presidency of the Federative Republic of Brazil.

Both aviation authorities have their own specific State Safety Program (SSP) by delegation of the Brazilian State as the *de jure* ICAO member state (Brasil, 2009). In fact, given the alleged successful experience of having two separate civil aviation authorities, Brazil has submitted for the approval of the ICAO High Level Safety Conference (ICAO, 2010) acceptance for having two safety coordinators in charge of Brazil's Universal Safety Oversight Audit Program (USOAP): DECEA and ANAC.

Notwithstanding, a 2009 audit by the local member of the International Organization of Supreme Audit Institutions (INTOSAI) found many overlapping rules regarding safety implementations (TCU, 2010). For clients of the aeronautical and airport infrastructures, regulations originating from two authorities double the administrative burden imposed by the many safety rules issued by these entities.

2.3. The Brazilian ANSP Organization

DECEA is a military organization under the Brazilian Air Command and linked to the Ministry of Defense. It is the only air navigation service provider and it is simultaneously responsible for Brazilian air defense and for Brazilian civilian airspace management. DECEA provides the services of aeronautical meteorology, aeronautical information, air traffic control and air traffic flow management. DECEA is also the main provider of accredited technical military and civil human resources. It has its own unit of military investigators of airspace control incidents and accidents, the Airspace Control Safety Advisory (ASEGCEA), with regional subunits spread around the country. The investigation team works closely with Brazil's Center for Accident Investigation and Prevention (CENIPA), another military organization.

DECEA's website points out that its organization is "distributed into three Subdepartments for supervision, four Integrated Centers for Air Defense and Air Traffic Control (CINDACTA), one Regional Flight Protection Service established in São Paulo (SRPV-SP), five Area Control Centers (ACC), 47 Approach Controls (APP), 59 Air Traffic Control Towers (TWR), 79 Regional Air Space Control Sections (DTCEA), in addition to more than 90 Aeronautical Telecommunications Stations and various support divisions across the country." (DECEA, 2014b).

Military organizations are based on strict discipline and also highly hierarchical with the organizational chart, invariably assuming the pyramid shape. This specific type grants managers huge control of the organizational processes for efficiency, due to the formal positions of authority and the superior knowledge people are expected to possess at higher ranks. Although in the pyramid-shaped organization "control" and "knowledge" are quite axiomatic, the military add rules that ensure blind and mechanical obedience.

Organizations structured on the pyramid model are conceptually known as bureaucratic organizations. Bureaucracy is the organizational face of rational thought, the essence of modernity. Bureaucratic organization is hierarchical, highly specialized, governed by clear rules and procedures, and impersonal." (Weber, 1946) And in Perrow's view:

> Bureaucratic organizations are the most effective means of unobtrusive control human society has produced, and once large bureaucracies are loosed upon the world, much of what we think of as causal in shaping our society -- class, politics, religion, socialization and self-conceptions, technology, entrepreneurship -- becomes to some degree, and to an increasing degree, and a largely unappreciated degree, shaped by organizations." (Perrow, 2002)

There are two other well-known broad types of government or business organizations besides the bureaucratic model: the matrix model and the team model but the bureaucratic model is the most used worldwide. This work will not discuss the pros and cons of these three business structure types as there is plenty of academic and non-academic literature on the subject. Our intent is to model a concept of an ANSP in accordance with systems theory with the goal of enhancing safety control and resilience (Hollnagel, 2006). In systems theory or control theory, systems are viewed as hierarchical structures where each level imposes constraints on the activity of the level beneath it -- that is, constraints or lack of constraints at a higher level allow or control lower-level behavior (Leveson, 2003). Also, the use of STAMP (Systems-Theoretic Accident Modeling and Processes) is expected to allow managers to more effectively detect hazards within the organization from the early design stage.

3. STAMP

The present study has as its main assumption that organizations prone to the loss of huge investments and/or many lives cannot be treated as any other organization with no such intrinsic characteristic. In general organizations of this type are highly automated, have more complex coupled subsystems, and also have the tendency to shift workers' duties from active roles to supervisory roles. Hence, organizations designed to have their management based on reliance on human decisions are gradually being substituted by organizations with reliance mainly on software decisions.

This fact necessarily drives us into a paradigm shift regarding the analysis of aspects of prevention of losses in these organizations. Here is where Systems-Theoretic Accident Models and Processes (STAMP) help designers and managers to get more comprehensive knowledge of their systems' safety than can it be acquired from traditional approaches. In fact, effectively preventing accidents in complex systems requires using accident models that include the social system as well as the technology and its underlying science. Without understanding the purpose, goals, and decision criteria used to construct and operate systems, it is not possible to completely understand and most effectively prevent accidents. (Leveson, 2004)

3.1. Safety and Reliability

Most traditional views on loss prevention (accidents) in complex systems link safety to the components' reliability: the more reliable the components of a given system, the safer the system. Nevertheless, safety and reliability are different system properties. As Leveson (2008) pointed out, one does not imply nor require the other -- a system can be reliable and unsafe or safe and unreliable. In some cases, these two system properties are conflicting, i.e., making the system safer may decrease reliability and enhancing reliability may decrease safety. In fact, accidents often result from interaction among perfectly functioning components.

3.2. Safety and Myths

Traditional views on loss prevention also influence or are recursively based on the common beliefs of government, regulators, prosecutors and accident investigators regarding safety. Even the word safety acquires several different meanings in accordance to the viewer's background. One example of a common belief is the traditional

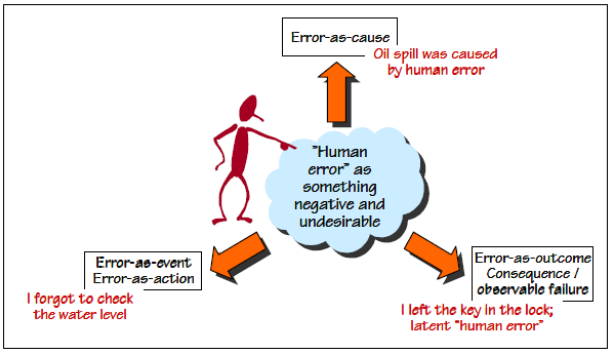


Figure 1 – Three connotations of the term "error" (Hollnagel, 2001)

dictum safety first. People tend to agree that

increasing protection will increase safety. Another belief is related to human error under the assumption that human error is the largest single cause of accidents and incidents, thus generating the losses of investments or lives. (Hollnagel, 2001).

Other beliefs, according to Hollnagel (2001), can be related to procedures compliance: The system will be safe if people comply with the procedures they have been given; root causes: Accident analysis can identify root causes (the 'truth') of why the accident happened; and even the accident investigation itself: Accident investigation is the logical and rational identification of causes based on facts. To these common beliefs we can add the retrospective vs prospective analysis: Retrospective analysis of adverse events is required and perhaps the best way to improve safety (Leveson, 2010).

3.3. Human Error

Being itself part of the common beliefs within the traditional view of loss prevention, the term *human error* has at least three different connotations: as a *cause*, as an *event* or *action* and as an *outcome* (Figure 1). For Woods (2003), *human error* is not a well-defined category of human performance. Attributing error to the actions of some person, team or organization is fundamentally a social and psychological process and not an objective, technical one. (Hollnagel, 2001).

Woods further explores the impact of the definition problems of *human error* on the common knowledge of *safety*:

> Nuclear power, aviation, manufacturing, and the military have invested heavily in basic and applied research on human error over the past 20 years. Although some of this research – and some outspoken researchers – rely on human error being a discrete, well circumscribed, static entity, progress on safety in these industries has come, in large part, from abandoning efforts to attack error" (Woods, 2003)

3.4. STAMP principles

In the STAMP conception of *safety*, accidents occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately handled by the control system, that is, they result from inadequate control or enforcement of safety -- related constraints on the development, design, and operation of the system. STAMP also provides a theoretical foundation for the introduction of unique new types of accident analysis, hazard analysis, accident prevention strategies including new approaches to designing for safety, risk assessment techniques, and approaches to designing performance monitoring and safety metrics. (Leveson, 2004)

Then, considering this system approach, safety becomes an emergent property of the system and it can only be well understood from the interactions among the components and/or subsystems within their specific environments. Systems theory fundamentals are these basic pairs of concepts: "emergence and hierarchy" and "communication and control".

As Leveson (2004) wrote:

> In systems theory, complex systems are modeled as a hierarchy of levels of organization, each more complex than the one below, where a level is characterized by having emergent or irreducible properties. Hierarchy theory deals with the fundamental differences between one level of complexity and another. Its ultimate aim is to explain the relationships between different levels: what generates the levels, what separates them, and what links them. Emergent properties associated with a set of components at one level in a hierarchy are related to constraints upon the degree of freedom of those components.

and

> In systems theory, control is always associated with the imposition of constraints. The cause of an accident, instead of being understood in terms of a series of events, is viewed as the result of a lack of constraints imposed on the system design and on operations, that is, by inadequate enforcement of constraints on behavior at each level of a socio-technical system.

The most basic concept in STAMP is "constraint" and STAMP should be useful not only in analyzing accidents that have occurred, but also in developing system engineering methodologies to prevent accidents.

> While STAMP will probably not be useful in law suits as it does not assign blame for the accident to a specific person or group, it does provide more help in understanding accidents by forcing examination of each part of the socio-technical system to see how it contributed to the loss (and there will usually be contributions at each level). Such understanding should help in learning how to engineer safer

systems, including the technical, managerial, organizational, and regulatory aspects. (Leveson, 2004)

4. ANSP CONCEPT

According to ICAO (2013b), an air navigation service provider (ANSP) provides services that comprise air traffic management (ATM), communications, navigation and surveillance systems (CNS), meteorological services for air navigation (MET), search and rescue (SAR) and aeronautical information services/aeronautical information management (AIS/AIM). These services are provided to air traffic during all phases of operations (approach, aerodrome and en route). The ultimate goal of an ANSP, whether state or privately owned, is the avoidance of aircraft collision within a given airspace jurisdiction, regardless of pilots and unmanned aircraft controllers' responsibilities. At the same time, the ANSP must prove itself to be efficient as a contributor of protection of the environment, and must also ensure the viability of the aviation industry while demands for air transportation tend to grow worldwide.

Separation of air traffic happens with the presumption that there is a minimally acceptable risk in the aviation industry regarding the design and the technology applied to its products, with the acceptance of Government entities. It also happens with the acceptance by the members of the

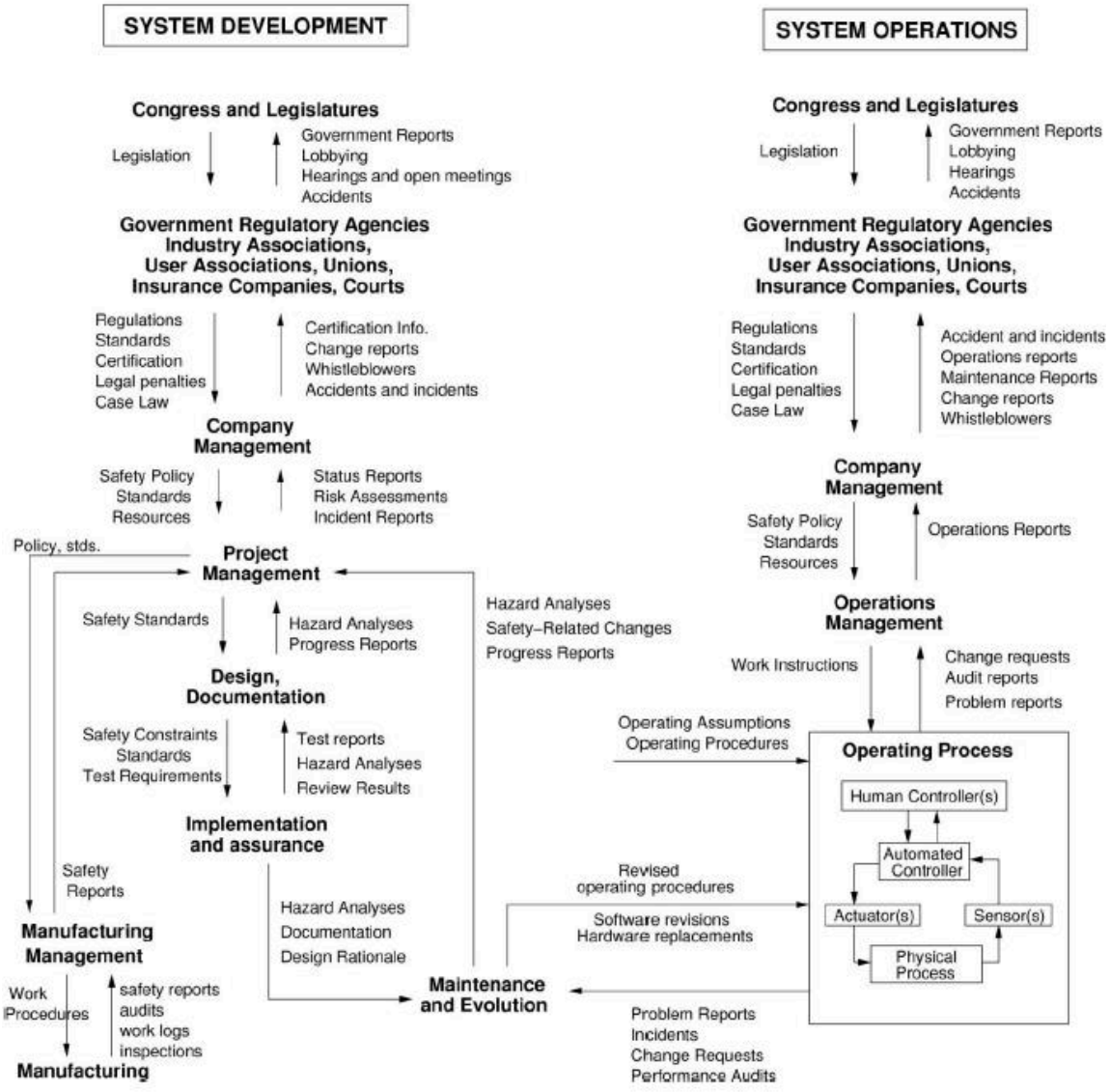


Figure 2 – General form of a model of a socio-technical control process (Leveson, 2004)

International Civil Aviation Organization (ICAO) of its standard recommendations and practices (SARP), not to mention the close surveillance of workers' unions and class associations. Feedback is of great importance for control process and for making adjustments to the system. Figure 2. shows a general form of a model of socio-technical control structure adapted by Leveson (2004) from the one devised by Rasmussen and Svedung (2000) in order to fit both systems operations and systems development.

The socio-technical control process seen in Figure 2 when applied to an ANSP led to the structure showed in Figure 3. In the left part of the picture the current system is depicted with processes mapped as we are likely to find in any ANSP worldwide. Adequate separation among aircraft in a controlled airspace is achieved by humans playing an active role in the air traffic control system. Clearance-based Operations (CBO) are the main safety constraints used to keep the air traffic separation within the acceptable risk of the State Safety Program (ICAO, 2013a). The air traffic controller issues instructions or vectors the aircraft to maintain the proper separation under a time-based management. Personnel are chosen by a filtering process that selects the necessary human abilities and develops the desired skills in the ab-initio course. The system is designed to send feedback to the management, regulators, and eventually to the international

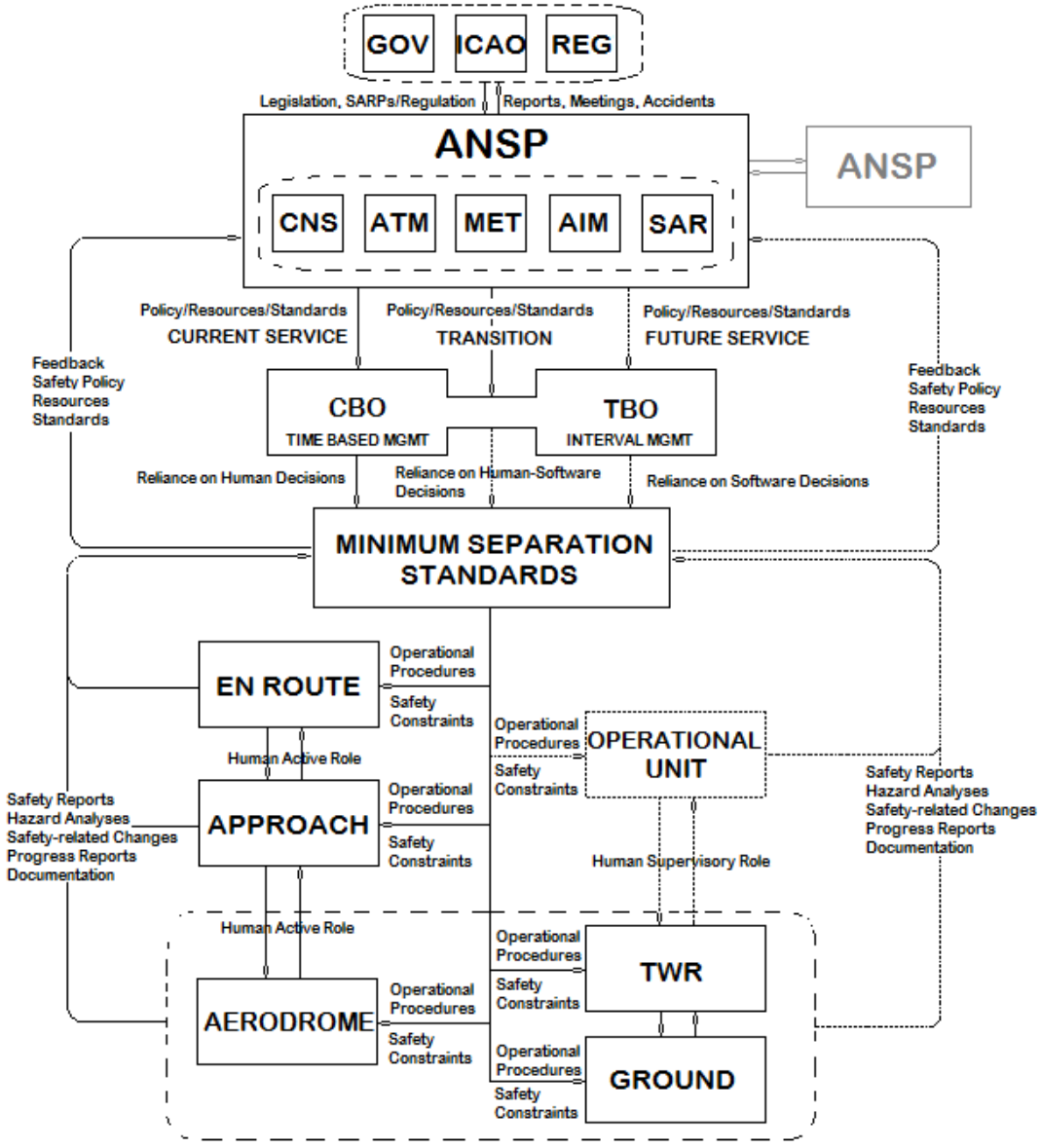


Figure 3 – Model of an ANSP socio-technical control process

organizations. It is also integrated with surrounding ANSP.

In the right part of the picture we managed to map the future ANSP. The goal remains the same: providing separation among aircraft in airspace. Whether the airspace will be controlled or users will perform a supervised self-control is an issue to be discussed on a further and more detailed work. Nevertheless we agree that some of the airport facilities will still remain the same, but operating them will be a little bit different than the usual approach at a certain extent.

4.1. Trajectory-based Operations (TBO)

Trajectory-based Operations (TBO) will keep the aircraft flying accurate 4D, i.e., space and time flightpaths, and as well "contract" those flightpaths with air traffic managers. TBO is not a continuous change building on the existing philosophy. It is disruptive innovation, a change to a "new paradigm" (Brooker, 2013). This new paradigm will efficiently optimize the airspace with more environment-friendly aircraft flying more direct routes using less expensive satellite-based navigation aids on a safer manner. In less than thirty years the ANSP will cope with the airspace dynamics integrating all the services provided with surrounding ANSPs, making the experience of flying different regions transparent to pilots.

4.2. ANSP socio-technical control process

In the center part of the Figure 3 it is shown the expected transition between the ANSP current and future services, CBO and TBO respectively. In this very phase none of them will be fully implemented and different policies and standards should be applied for both workers and users. Human abilities, the developed skills and the training process must deal with both worlds simultaneously. STAMP comes with a tool for helping designers to prevent hazards while still in the designing process. In STAMP system is not treated as static but as dynamic processes that are continually adapting to achieve their ends and to react to changes in themselves and their environment (Leveson, 2011).

4.3. ANSP Analysis Tool

The tool System-Theoretic Process Analysis (STPA), part of the STAMP, was created to provide a more comprehensive and effective manner of detecting complex systems hazards. Its goal is to identify safety constraints/requirements necessary to ensure acceptable risk, as any other hazard analyses tool. The difference found is that throughout an iteration process STPA accumulates information about how hazards can be violated, which is used to eliminate, reduce and control hazards in system design, development, manufacturing, and operations. STPA also supports a safety-driven design process where 1. hazard analysis influences and shapes early design decisions and 2. hazard analysis is iterated and refined as design evolves. (Leveson, 2012)

5. CONCLUSIONS

Trajectory-Based Operations (TBO) is far from being just an evolution from the current Clearance-Based Operations (CBO) concept used by air navigation services providers worldwide to provide an airspace safe environment. TBO is a brand new concept that must receive special attention from governments, aviation authorities, industry, and the various working class associations among other stakeholders. ANSPs preferred organizational chart has been the pyramidal one, or the rational-bureaucratic organization. Highly hierarchical and bureaucratic management allows better human control by managers and it is also believed to keep the operational work within the safety boundary of the "work-to-rule" protocol in order to avoid the assumption that human error has been documented as a primary contributor to more than 70% of the airplanes hull-loss accidents (Boeing, 1999).

In this view the human part of the system is treated as a system component meaning that although humans are part of the socio-technical environment they are analyzed in terms of their performance and not rare apart from the whole system.

Meanwhile, industry seeks to develop a more safe work environment -- hence operations -- by adding automation where humans are expected to fail more as indicated by statistics and quality assurance audit. Thus, following these philosophies that provide an administrative comfort zone, ANSPs implement a patchwork of different integrated systems with the sole intention to avoid "human error", simultaneously enhancing the system reliability and providing more situational awareness, as they understand it.

If TBO is a brand new way of doing air navigation services, the problem lies on how to provide an adequate control in the form of enforcement of the safety constraints on the system behavior in its early stages of development. STPA, or Systems-Theoretic Process Analysis, comes to help as a new hazard analysis technique with the same goals as any other hazard analysis technique but with a very different theoretical basis or accident causality model. STPA is a tool developed to identify scenarios leading to identified hazards and thus to losses so they can be eliminated or controlled. This also includes the ANSPs in countries which use a patchwork of technology for their financial resources to invest on a systemic solution integrated to the surrounding ANSPs -- and in accordance to a global agreement (ICAO, 2013c) -- are highly compromised by governments' priorities.

The Brazilian accident over the rainforest back in 2006 acted as the trigger to evaluate the way the current concept of air navigation services are being provided in Brazil. This article proposes further works using the new hazard analysis technique based on STAMP causality model, called STPA (System Theoretic Process Analysis), to assess the safety of the current air navigation services providers using CBO. It also proposes a special attention to the CBO/TBO transition phase onward.

6. REFERENCES

ANAC - http://www2.anac.gov.br/portal/cgi/cgilua.exe/sys/start.htm?sid=330 last access in 23/07/2014

BOEING - **The Role of Human Factors in Improving the Aviation Safety**, Aero Nº 08**,** QTR_04 1999 http://www.boeing.com/commercial/aeromagazine/aero_08/human.html last access in 23/09/2014.

BRASIL - Brazil Safety State Program (SSP) - **PSO-BR Portaria Conjunta nº 764/GC5**, de 14/08/2009

Brooker, P. - **4D-TRAJECTORY ATM** - Air Traffic Technology International, UKIP, 2013, pp 6-12.

CENIPA - **Final Report: N219AS 19 Sep 1986**, 29th Feb, 1988

CENIPA - **Final Report: PR-GTD_N600XL29 Sep 2006**, RF A-022/CENIPA/2008

DECEA (2014a)- http://www.decea.gov.br/en/index.php?i=about accessed in 14/07/2014

DECEA (2014b) - http://www.decea.gov.br/en/index.php?i=structure last access in 31/07/2014

Hollnagel, E; Amalberti, R. - **The Emperor's New Clothes Or**

Whatever Happened To "Human Error"?, 2001.

Hollnagel, E.; Woods, D. D.; Leveson, N. G. - **Resilience Engineering: Concepts and Precepts**, Ashgate Publishing, 2006

ICAO Doc 7300 - **Convention on International Civil aviation** – Montreal, Canada – 7th December 1944

ICAO - **Brazil WP HLSC.10.WP.055.1**, High Level Safety Conference, 2010

ICAO - Annex 19 - **Safety Management**, 1st Ed., 2013a

ICAO - Doc 9161 - **Manual on Air Navigation Services Economics**, 5th Ed., 2013b

ICAO - Doc 9750 - **Global Air Navigation Plan (GANP)**, 4th Ed., 2013c

Leveson, N. G.; Daouk, M.; Dulac, N. ; Marais, K. - **A Systems Theoretic Approach to Safety Engineering**, MIT, October 30, 2003

Leveson, N. G. - **A New Accident Model for Engineering Safer Systems** - Safety Science, Vol. 42, No. 4, April 2004, pp. 237-270

Leveson, N. G. - **Applying Systems Thinking to Analyze and Learn from Events** - Safety Science,Vol. 49, No. 1, January 2010, pp. 55-64

Leveson, N. G. - **Engineering a Safer World: System thinking applied to safety**, MIT Press, 2011

Leveson, N. G. - **STPA: A New Hazard Analysis Technique, 1-2-Beginners-Tutorial-part2**, PPT, 2012

Perrow, C. - **Organizing America**, Princeton University Press, 2002 p.4

Rasmussen, J., Svedung, I. - **Proactive Risk Management in a Dynamic Society**, Swedish, Rescue Services Agency, 2000.

TCU - **Relatório de Auditoria de Natureza Operacional ANAC/INFRAERO/DECEA/CENIPA**, Tribunal de Contas da União Código eletrônico AC-1103-16/10-P, 2010

Weber, M. - Essays in Sociology, 1946 apud Jaffee, David - **Organization Theory: Tension and Change**, McGraw-Hill, 2001, p 111.

Woods, D. D.; Cook, R. I. - **Mistaken Error**, in M. J. Hatlie and B. J. Youngberg (Eds.) Patient Safety Handbook, Jones and Bartlett, 2003.