Limitations of systemic accident analysis methods

Casandra Venera BALAN (PIETREANU)*[,1], Valentin-Marian IORDACHE[1]

*Corresponding author
[1]"POLITEHNICA" University of Bucharest, Aerospace Engineering Department,
Polizu Street 1-7, sector 1, Bucharest 011061, Romania,
casandra.pietreanu@yahoo.com*, valentin.iord1504@gmail.com

DOI: 10.13111/2066-8201.2016.8.4.14

Received: 03 October 2016/ Accepted: 07 November 2016/ Published: December 2016

International Conference of Aerospace Sciences "AEROSPATIAL 2016"
26 - 27 October 2016, Bucharest, Romania, (held at INCAS, B-dul Iuliu Maniu 220, sector 6)
Section 8 – Management in Aerospace Activities

Abstract: *In terms of system theory, the description of complex accidents is not limited to the analysis of the sequence of events / individual conditions, but highlights nonlinear functional characteristics and frames human or technical performance in relation to normal functioning of the system, in safety conditions. Thus, the research of the system entities as a whole is no longer an abstraction of a concrete situation, but an exceeding of the theoretical limits set by analysis based on linear methods. Despite the issues outlined above, the hypothesis that there isn't a complete method for accident analysis is supported by the nonlinearity of the considered function or restrictions, imposing a broad vision of the elements introduced in the analysis, so it can identify elements corresponding to nominal parameters or trigger factors.*

Key Words: *Accident analysis, Systemic methods, STAMP, FRAM*

1. INTRODUCTION

Designed safety requires knowledge, understanding of the environment and stakeholders/involved factors and is not based on formal identification of threats and vulnerabilities of a system, but on analysis that requires increased performance, technology development and levels of safety. Airborne systems have a particular structure, but similar to other systems, their inadequate operation leads to the possibility of a failure of a structural element or of the system as a whole. Therefore, if we treat the problem of risk, in order to keep it at a low/acceptable level, control structures should be implemented in the early stages, starting from the design phases [1].

In the context of 8727691 commercial flights in 2015 and 23911 each day, 2246004 passengers travel daily by 7523 commercial aircraft to 19 299 airports in the world. The entire spectrum of major accidents overlaps 5 classes that allow analysis of existing threats, causal relationships and ultimately identify the causes of accidents (human factors, organizational, faulty assumptions, unintentional or latent errors) [10]. In parallel with developments in technology, a series of interconnected systems vulnerabilities have been outlined as a cobweb pattern. Starting from the first development of accident modeling tools in the early 1930s, which mirrored in a simplistic manner, a linear extension of the causes of an event in its results and consequences, subsequent exposures experienced a progressive evolution by developing rigorous mathematical models built at the base of exhaustive playing of the systematic factors and nonlinear interactions between them. Therefore, the imposition of an abstract accident exposure through a descriptive understanding of an accident's stages (through the Domino model) and shaping as a way of unraveling and conceptual figurative solving of a critical situation by canceling or removing one of the pieces of the assembly, imposing barriers and adequate control to each process type and each category of possible error has become an important custom for which a dispensation is not considered [1]. In 86 years of evolutionary study upon considerations that highlight a wide range of processes whose unplanned interactions can reflect in an accident, corresponding stages of progress achieved follows a technical-systemic line with frequent imposition of human factor and, by extension, an organizational alternative. The need to understand the complexity of human error was driven by the failure to further explain accidents by simple cause-effect chaining and the fact that accidents involve successive penetration of the defense lines of the system; therefore the event modeling is useful to highlight potential risks, to assess and implement actions designed to prevent occurrence of other accidents [9].

2. CHARACTERISTICS OF SYSTEMIC METHODS. A NONLINEAR APPROACH

Analytical models must reflect the research in the area and the results of safety investigations, describe the system's performance by establishing connections between functions and components of the analyzed assembly and monitor performance variation as a means of control. The field of events modeling includes the category of organizational accidents with multiple causes involving the human factor (acting at different levels of the company concerned); they occur due to the existence of modern complex technologies and often have catastrophic consequences because they are a product of technological innovations that have radically changed the relationship between systems and human elements [3].

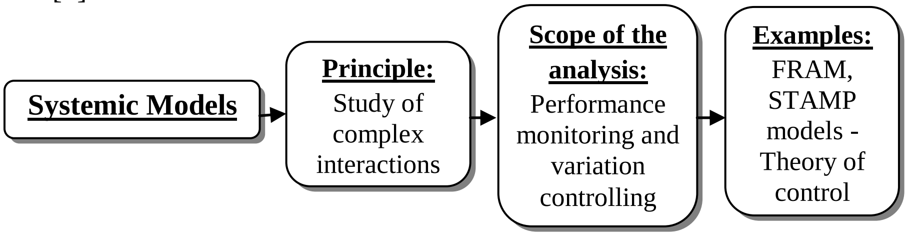


Figure 1. Organizational evolution of safety culture

Systemic models highlight the possibility and meaning of unforeseeable occurrence of complex combinations of events and understanding interactions of the structural elements of the system by studying the influences and associated effects.

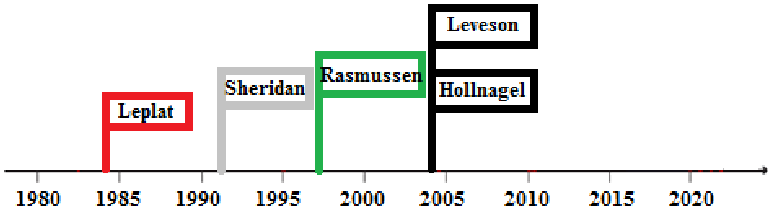


Figure 2. Research on system theory

Systemic methods have evolved sinuously. Their evolution was accelerated in the last decade by Leveson and Hollnagel’s proposals (2004), employing many sub-systems and processes in an exhaustive analysis that outline the involvement and performance of the human factor. Thus, the research of system entities as a whole is no longer an abstraction of a concrete situation, but an overtaking of the theoretical limits set by analyzes based on linear methods [1].

The study of events amid processes automation is incomplete unless it takes into account the nonlinear behavior defining human factor and the environment of accident occurrence.

So, in terms of system theory, the description of complex accidents is not limited to the analysis of the events sequences/individual conditions, but emphasizes the non-linear functional characteristics and frames the human or technical performance within the normal functioning of the system in terms of safety.

$$P.O.\begin{cases} \min f(x), & x \in \mathbb{R}^n \\ g(x) \leq 0, & g(x) = (g_1(x), g_2(x), \dots, g_m(x)) \\ x \geq 0 \end{cases} \tag{1}$$

Considering the optimization problem exposed above, the allowable solutions will be found in the set:

$$PM = \{x \in \mathbb{R}^n | g(x) \leq 0 \Leftrightarrow g_1(x) \leq 0, g_2(x) \leq 0, \dots, g_m(x) \leq 0, x \geq 0\} \tag{2}$$

The variation on analyzed processes and system performance is a source of nonlinearity; they may have different values and alterations in relation to certain factors or influences. The context or risk awareness, a good knowledge of the system, improvement of certain processes, establishment of a strict control and a thorough preparation will limit the oscillations.

Modeling such matters as a means of optimization will be carried out by limiting the influence factors or the performances analysis of the system without causing major changes which would imply error in calculations or erroneous approach to the issue.

$$f(x^*) = min\{f(x), x \in \mathrm{M}\} \tag{3}$$

In conclusion, systemic approach of accidents in the context of a malfunction, external perturbations or interactions between the system components that are not managed properly, implies control issues on the aspects listed above with repercussions on understanding the causes of an accident and errors in determining the cause for which the control was ineffective [5].

3. CRITICAL ANALYSIS OF SYSTEMIC METHODES. DEFINING FEATURES AND HIGHTLIGHTING THE LIMITATIONS OF STAMP AND FRAM MODELS

System accident investigation methods (through system theory) aim understanding the application field, its capacity and possible use by practitioners, by highlighting their strengths but also their limitations.

Comparative study of STAMP and FRAM methods is supported on the one hand by the common characteristics that come from belonging to systemic methods class, by methodologies on which they stand, and on the other hand by their distinct development.

It is therefore considered that it can be applied in a synergistic way for an extended nonlinear analysis that provides conclusive solutions [1].

The study of accidents with theoretical references and analysis of processes has pursued an imprecise development but with great chances of success through operational and technical perspectives on issues discovered in preeminent levels of the concepts found in Rasmussen's method descriptions.

STAMP is based on a series of concepts that describe the systems through the control scaling, supported by feedback mechanisms and analysis phases concerning the construction of the hierarchical structure of control by analyzing restrictions amid interactions of functional components and error study preceded by control imposing [2].

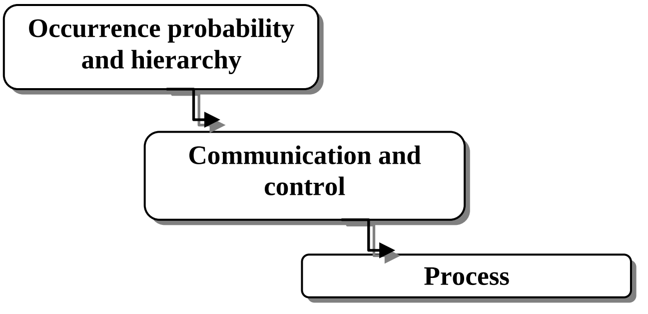


Figure 3. STAMP process analysis model

The 2011 validation of the method with nonlinear features did not conclude the evolutionary stages that treat changes in the systems and environmental influences, applicable constraints and adaptability to abnormal conditions.

Within seven years, the conversion of formal introduction into implementing structural mechanisms of the method “System-theoretic Accident Model and Process”, envisages adjustments on assessing dynamic equilibrium of the systems and discerning the manner in which insufficient control will converge to circumstances altered by system failures [1].

The attribute of restrictions on control problems represents a focal point of the instrument proposed by Nancy Leveson.

Emergent factors treatment requires the application of barriers and restrictions in order to control and understand indications regarding changes in the levels of safety [6]. In this manner, if the implementation of constraints is made correctly, the errors will be limited and their discovery becomes easy whereas it requires restricted analysis, thus excluding the magnitude of total lack of control case analysis.

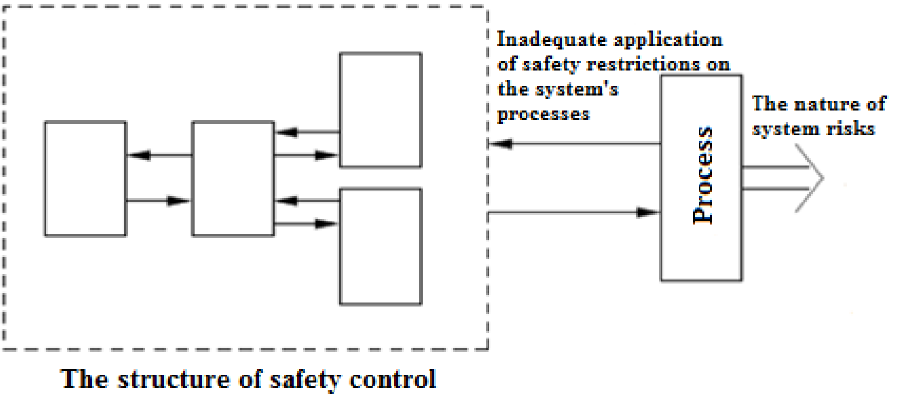


Figure 4. STAMP causal model

The functions that fail in the effort to preserve/not modify the safety levels analyzed before an accident, outline the accident scenario, highlighting the chronological evolution and hierarchical performance.

A dynamic reconstruction of the environment interaction with the entire technological/human ensemble will build a critical analysis of processes, actions and central stages directed towards the loss/cancellation of control barriers [1].

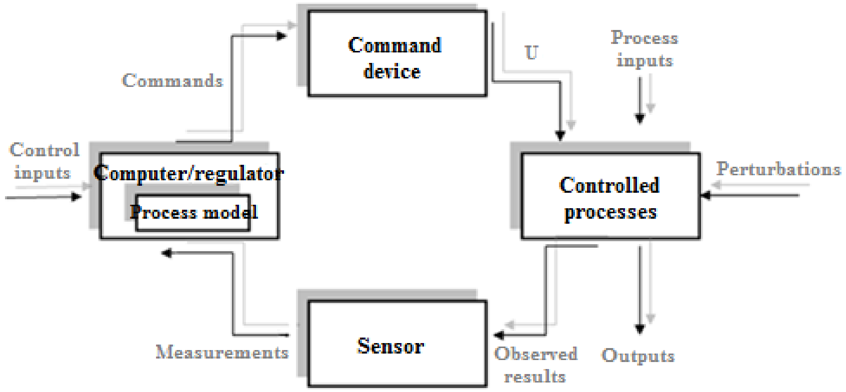


Figure 5. STAMP process control loop

The limitations of this method also relate to its practical implementation, not just the theoretical application. In this sense, covering the issues of interest in literature is not defining or complete for the validation of methods; the difficulty to set directions to assess the lack of control, the absence of proper guidance or feedback on the method and an insufficient definition of the elements, confirm the hypothesis that there isn't a complete data analysis method. FRAM analysis proposed by Hollnagel in 2004, aims the perception of fluctuations effects repercussion mechanism at the performance level via functions or actions that induce nonlinear propagation hard to evaluate, making a parallel of the processes evolution to specific-ordinary situations [8].

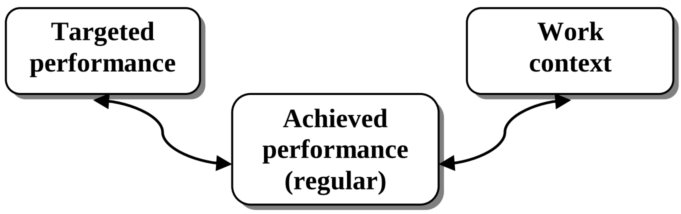
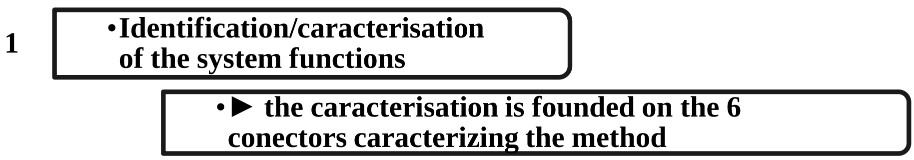


Figure 6. Variation in function performance

Entities and issues covered by this model do not particularly target structural components of the system and the functional ones in relation to these, the method focusing on circumstances and conditions which converge to an accident.



The nonlinear approach is also found in the "Functional Resonance Analysis Method", analyzing nonlinear functions and (possibly nonlinear) restrictions whose aspects and values determine the structure of a node.

2 **•Characterizing the potential variation**

•► is achieved by means of a checklist

In the described context, it is natural that the adopted procedures be suitable (or at least adjustable) to functional coupling in order to minimize damage and maximize the precision of perception in this circumstances.

3 **•Definning functional resonance**

• ►is achieved by shaping the functions subordination in relation to performance variation

As expected, the variation of a greater number of features and connections between them involve proportionate consequences, often unpredictable, entangling the analysis which leads to increased risks [1].

Performance conditions useful to functional resonance defining, aim organizational aspects, technological and human factors. Subsequently for their identification, qualitative change in the system must be determined in terms of stability, predictability and performance limits [4].

The method solves an important matter that which should not only focus on the man-machine connection; highlighting the influence of the environment by defining the characteristic noise and consequences of performance oscillations enables modeling the system entities interactions in a way different from that of Nancy Leveson, by reference to a specific (normal) situation.

4 **•Setting barriers**

• ► is achieved through continuous observation and monitoring of performance variance

By imposing barriers at micro level or overall, is developed a chain process that can overturn accidents or eliminate their effects and random unpredictable aspects, making subsequent analysis with predictive aspects.

The practical aspects of functional resonance model (with a very complex structure) are useful for application in various fields, but the issues and perception of problems/errors cannot be resolved by this method; however, it may indicate the procedure to uncover systemic factors [1].

4. COMPARATIVE STUDY OF STAMP AND FRAM MODELS WITH LINEAR ACCIDENT ANALYSIS METHODS

Probabilistic approaches on reliability that aim an optimal insight of risk probability by producing malfunctions, can be supported by a systemic assessment of the analysis and examination of alternatives for solving this problem.

The optimization of the linear analysis itself (which will seek as appropriate, maximize results and safety levels, or risk/errors/malfunctions minimization) is insufficient when considering determinant systemic factors in an implementation, maintenance, improper operating or insufficient functional or symbolic barriers framework [1].

$$
\begin{gathered}
f = c_1x_1 + c_2x_2 + \cdots + c_nx_n \\
f: \mathbb{R} \to \mathbb{R}^n \\
\begin{cases}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \geq b_1 \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \geq b_2 \\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \geq b_m \\
\quad x_i \geq 0, \qquad i = 1 \dots n
\end{cases} \\
A = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{bmatrix}, \quad A \in M_{m,n}(\mathbb{R}) \\
b = \begin{bmatrix} b_1 \\ \dots \\ b_m \end{bmatrix}, \; m \in R^m \\
x = \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix}, x \in R^n \\
c = [c_1 \dots c_n] \,, c \in R^n \\
f(x^*) = \min(f(x))
\end{gathered}
\tag{4}
$$

Analyzes on aviation events should not be limited to a linear approach aimed to model independent failures, a research completed eventually through a hierarchy of error classes; this view is not incorrect as a whole, but is unsatisfactory and confines extensive research that takes into account the system oscillations. The nonlinearity of the function or restrictions imposes a broad vision of the elements introduced in the analysis.

Optimization problems with linear restrictions and nonlinear objective function have an impact on the accuracy of understanding and managing specific vulnerabilities, modeling with high precision the analyzed situations, sometimes by imposing additional conditions to the function or restrictions of the problem and approximating with accuracy the original nonlinear objective [7].

$$
f(x_1, x_2, \dots, x_n) = c_0 + \sum_{i=1}^{n} c_i x_i + \sum_{1 \le i \le j \le n}^{n} c_{ij} x_i x_j \tag{5}
$$

Accidents examination from a systemic perspective should reflect the reality as accurately as possible, because systemic factors may affect control, defense structures against failures and functioning of barriers.

An increased attention should be directed to the human factor, taking into consideration that minimizing its role in addressing issues of safety can be regarded as a failure in itself.

5. CONCLUSIONS

The limitations found in the last generation nonlinear methods show lack of guidance for practical application, this way limiting a broad perspective on the context, involved factors, and thus a proper analysis of system interactions. The conflict on expertise and training and the required effort to be implemented by experienced users should be based on extensive theoretical knowledge.

By addressing errors in a systemic way and analyzing the magnitude of the conditions of an accident, the defining elements of the proposed analysis can be found in a combination of characteristics and limitations of nonlinear methods and other original proposals that implement concepts and notions from exact sciences range but also social and psychological aspects and mechanisms related to learning and implementing human decisions and actions.

The analyzed events, classified corresponding to the evolution of causal factors must be considered from a starting point corresponding to a flight phase or a critical moment that triggers an action/erroneous decision and will be described through a series of control functions. In order to maintain a low (acceptable) risk, control structures should be implemented in the early stages, since the design stages [1].

REFERENCES

[1] C. V. Bălan (Pietreanu), *Contribuţii la dezvoltarea metodelor de analiză a accidentelor de zbor*, PhD Thesis, July 2016.

[2] N. G. Leveson, *A new accident model for engineering safer systems.* Massachusetts Institute of Technology, Aeronautics and Astronautics, SUA, 2002.

[3] J. Reason, *Human error*, Cambridge, UK: Cambridge University Press, 1990.

[4] L. Macchi, E. Hollnagel, J. Leonhard, *Resilience Engineering Approach to Safety Assessment: An Application of FRAM for the MSAW system*, Crisis and Risk Research Centre, MINES ParisTech, https://hal-mines-paristech.archives-ouvertes.fr/hal-00572933, Submitted on 2 Mar 2011

[5] V.-. Iordache, C. V. Balan (Pietreanu), Safety Culture in Modern Aviation Systems – Civil and Military, *INCAS BULLETIN*, Volume **8**, Issue 2, pp. 135 – 142, (online) ISSN 2247–4528, (print) ISSN 2066–8201, ISSN–L 2066–8201, DOI: 10.13111/2066-8201.2016.8.2.11, 2016.

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

[7] I. Slavici, *Rezolvarea numerică a problemelor de optimizare, Matematici asistate de calculator*, Note de Curs.

[8] E. Hollnagel, O. Goteman, The Functional Resonance Accident Model, In *Cognitive Systems Engineering in Process Control*, 2004.

[9] C. Perrow, *Normal accidents: Living with high risk technologies,* ISBN: 9780691004129, 464 pp., eBook ISBN: 9781400828494, 1999.

[10] * * * www.faa.com