ASPECTS REGARDING THE USING OF STOCHASTIC INGREDIENTS IN THE PROCESS OF ACCIDENTS MODELING – THE CASE OF SAFETY ENGINEERING SYSTEMS

Cătălin CIOACĂ*, Elena Corina BOŞCOIANU**

*"Henri Coandă" Air Force Academy, Braşov
**Transilvania University of Braşov

Abstract: *The analysis of factors contributing to accidents and the deep understanding of the correlations between these factors allows, on the one hand the emergence of building an explanatory framework of accidents occurrence, and highlights strategies and tactics to prevent possible incidents in the future. For the construction and implementation of safety systems one must consider all causative factors (direct and indirect) and the interrelationships between them. Specific mechanisms of accident patterns significantly affect the ability to identify and control hazards and thus prevent accidents. The results obtained by simulating the dynamics of costs and benefits, as a Wiener process with jumps modeled using Poisson distribution, is a complete solution for improving decision making in high technical systems.*

Keywords: *safety engineering systems, accident models, geometric Brownian motion, Poisson process*

1. INTRODUCTION

Understanding the mechanisms that contribute to accidents in complex socio-technical systems is extremely difficult due to complex interactions between component systems and processes dynamics.

In order to substantiate the occurrence of accidents explanatory framework that allows highlighting strategies and tactics to prevent possible incidents in the future an analysis of causal factors (direct and indirect) and the correlation between them is critical.

The analysis of the mechanisms of accidents occurrence in complex socio-technical systems in the context of complex interactions at the level of components can start from principles of systems engineering [1, 2] which provides an upper multiple perspectives and building upon the foundations of data and information specific to large and complex systems.

Sage highlighted the problem of scalability [3], Blauberg and Haimes evoked multidimensionality essential principle in understanding technical interactions with socio-human factors [4, 5].

Subsequent analyzes focused on a new discipline, namely safety engineering systems, beginning at the following generic hypotheses:

- impressive rate of technological change (which reduces the power of lessons learned, and introduces new elements of uncertainty);
- changing nature of incidents and accidents with the emergence of new types of hazards;
- reducing the ability of fructification of previous experience (by reducing capabilities and test periods);
- reduced tolerance for accidents in the context of more complex dynamics;
- the emergence of new difficulties in prioritizing the new aggressive and competitive backgrounds;
- the changing nature of the complex relationships between human factors and automation (resulting new types of human error related to inadequate human-machine communication);
- the dynamics of change and visions regarding safety regulations creates self sustainable imbalances.

2. MODELS OF ACCIDENT DEVELOPED USING SAFETY ENGINEERING SYSTEMS

One must first mention the existence of confusion about the concepts of safety and reliability.

In a context where most accidents arise from the interaction between system components and not the failure of individual components different situations should be taken into account: reliable, but insecure or unsure, but unreliable.

If reliability suggests an average lifetime between two failures, safety concerns the lack of accidents involving not necessarily the increase of the reliability of components and the increase of system security. In addition, socio-organizational levels fall to other levels different from physical systems [6].

Second, accidents are caused by chains of interdependent events and accident models should be designed not only to explain the causes of occurrence, but to offer prevention approaches.

In classical models a universal set of typical mechanisms is considered, which influences the results in the ability to identify and control hazards and thus prevent future accidents.

The first models in which integrated the socio-component were the domino management models [7], these management models are inadequate for complex socio- technological systems as they fail to identify human errors within accident processes.

Chain type models or multiple synchronized chains are based on safety engineering systems but suffer from problems of linear causality that can not be incorporated into the current highly non-linear phenomena, namely the difficulty selection and hierarchy of events that can be subjective.

The chains of events focus on past events, neglecting some relevant mechanisms.

The new models should provide an extended vision beyond causal factors that takes into account the conditions that allowed the appearance of the event or the indirect factors.

In multi-level approaches, Johnson proposed a model of systemic, contributory and direct factors such as the checklist method MORT (management oversight risk tree) [8] and Rasmussen-Svedung proposed a structure in which explicit social factors are detailed [9].

Assigning historical probabilities to PRA methods (probabilistic risk assessment) wrongly considered as mutually-exclusive events, does not describe the actual conditions in which the probabilities were assessed and thus they can not provide guidelines on the role of organizational and management factors [10].

Regarding the conflict between the flawed design and human errors the subjective temptation of overestimation of the role of the operator as the final element in the chain of events exist, including in interventions at limit of the functionality, alongside with the underestimation of the error of conception.

In order to provide a more accurate picture of the actions/decisions of the operator is essential to avoid the improvidence bias sites (to simplify the causality analysis by anchoring an initial hypothesis; overestimation of the role of rules/ procedures; superficial analysis of data relevance, over-correlation of results with previous actions) [11].

In the literature there is a tendency to treat errors of the human factor similar to physical fall of components/subsystems mechanisms, based on the simplistic idea of deviation from nominal specified or prescribed performance.

Approaches to the human factor are much more complex. Instructions and procedures are always on senso-stricto, as operators try to be more efficient and productive under the pressure of time. Thus, violation of rules shows some level of rationality [12].

The new mental models should include perceptions differentiation of designer - operator.

During development, the designers create their ideal model, significantly different from the real system built and used. The designer aims the integration of standard operators and this is actually the starting point in the development of work instructions and training programs or courses.

Moreover, the issue is complicated because there are differences due to structural diversity and evolution in time. The operator reference model starts from the model devised by the designer and seldom includes user experience.

Although formal procedures, work instructions and training are amended and updated periodically in order to reflect operating environment, there is always a delay. In addition, the operator is often working under time pressure and the productivity rules do not always reflect considered ideal procedures [13, 14].

Along with the maturation and evolution of the system, operators use feedback to update their mental models. Operators are involved in experimentation and learning processes in the borders of safety.

The experimentation is essential in change management and may lead to re-assess response to unexpected situations. As a result, designers' models are more simplistic than those of the operators, but usually all operators are liable even if the decisions were based on incorrect information processed reasonably at the time.

Feedback and experiments are essential elements in convergent mental models.

3. THE ANALYTICAL MODEL FOR ASSESSING THE SAFETY INVESTMENTS

Using the discrete time version of the geometric Brownian motion model allows the analysis of the accidents process and identifies management solutions leading to prevention disposals.

Multiple sources of risk jump are considered independent of each other, each having randomly size and jump timing (Poisson distribution) [15].

In designing a complex socio-technical system, each subsystem/component corresponds: direct costs (ie. acquisition, operation, maintenance, modernization, insurance), indirect or intangible costs (eg. giving up safety checks under efficiency and productivity pressure) and benefits (eg. reducing the number of accidents).

The current recognized value of the socio-technical system can be determined by the rate of increase/decrease expected in time related dependence assumptions and constant volatility (eq. 1).

$$\frac{dS}{S} = \mu \cdot dt + \sigma \cdot dz \tag{1}$$

In equation (1), S represents the value of the entire socio-technical system and is composed of and technical factor value S_1 and the human factor value S_2; $\mu_{1,2}(t)$ is the yield of each component in function of time, σ is the volatility, and z follows a Wiener process.

Consider the situation where S_2 (value of human resource insurance) accounts for 25% of the technical factor S_1 at time t_0 (eq. 2).

$$S = \sum_i S_i = 100 \quad \text{(monetary units)} \tag{2}$$

It exemplifies the following possible situations. For S_1, based on the models of reliability theory, it is considered a volatility of 20% per annum with -7% yield, and an initial value 80 monetary units. For S_2, based on theories of return on human factor is considered the volatility of 20% per year with 10% yield and an initial value 20 monetary units.

If ΔS_1 represents the fluctuation of the technical value and ΔS_2 is the fluctuation in the human factor in the next short period of time Δt, then equation (1) becomes (eq. 3):

$$\frac{\Delta S_1}{S_1} = -0{,}07\Delta t + 0{,}2\Delta z \tag{3}$$

$$\frac{\Delta S_2}{S_2} = 0{,}1\Delta t + 0{,}2\Delta z$$

The variable z follows a Wiener process, so Δz can be written as $\varepsilon\sqrt{\Delta t}$, where ε is a random variable with standard normal distribution. For a period of 30 days (Δt=1/12=0,083) equation (2) and (3) become (eq. 4):

$$\Delta S_1 = -0{,}00581 \cdot S_1 + 0{,}0576 \cdot S_1 \cdot \varepsilon_1 \tag{4}$$

$$\Delta S_2 = 0{,}0083 \cdot S_2 + 0{,}0576 \cdot S_2 \cdot \varepsilon_2$$

Using Monte Carlo simulation, values for the random variables ε_1 and ε_2 are generated using the inverse cumulative normal distribution. Thus, the evolution of the values of the two factors is obtained (figure 1a and 1b).

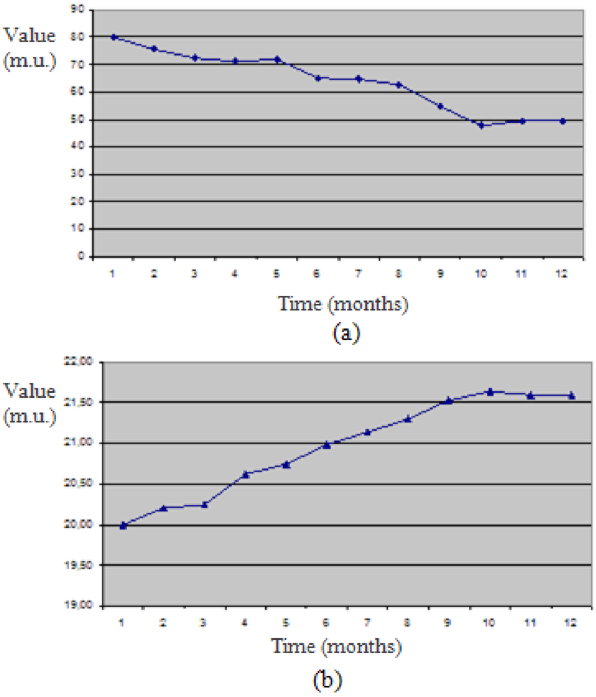

Fig. 1 Value of insurance
(a) Technical factor
(b) Human resource

Although there are limitations on the extension of these methods of calculation, management can not ignore the need to adapt to the new permanent organization of the market in order to remain competitive.

For the proposed model, evaluation of costs (C) is carried out on three components: insurance costs (C_a), maintenance costs (C_m) and acquisition, repair and upgrade (C_{aru}) (eq. 5).

$$C = C_a + C_m + C_{aru} \qquad (5)$$

The insurance costs associated with technical and human factors are aggregated according to equation (6), where α_1 and α_2 are the insurance premium (figure 2).

$$C_a = \alpha_1 \cdot S_1 + \alpha_2 \cdot S_2 \qquad (6)$$

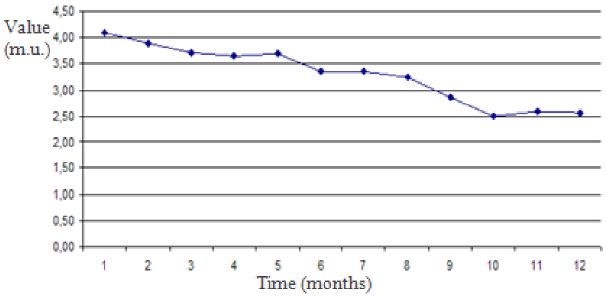

Fig. 2 The evolution of insurance costs

The costs of maintenance (corrective and adaptive) associated with regular work are determined by a similar algorithm with insurance costs to an initial value of 100 monetary units (maintenance costs are comparable in value to the cost of high-tech systems acquisition), which considers volatility of 20% per year with yield of 20% (figure 3).

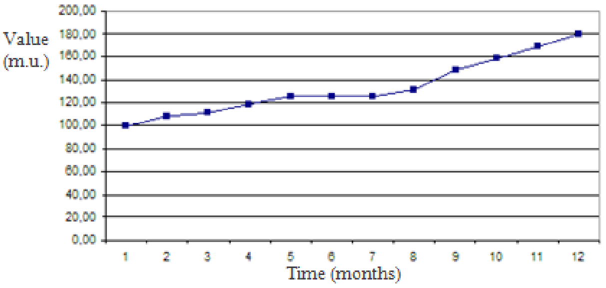

Fig. 3 The evolution of maintenance costs

Acquisition, repair and upgrade costs are evaluated in terms of the possibility of accidents. Positive jumps, whose source is the technical failures, are uncertainties about the timing and consequences of such events. The assessment of these costs with multiple risk sources (Brownian motion) and evolution described by a Markov chain is performed using equation (7).

$$C_{arm_{t+1}} = \eta \cdot C_{arm_t} + \sigma \cdot C_{arm_t} \cdot \xi \left[1 + \sum_{q=0}^{i} \left(e^{-\lambda} \frac{\lambda^q}{q!} \right) \right] \qquad (7)$$

In the cost equation (7), η is the growth rate per unit time and is calculated based on yield μ, according to equation (8), σ is the volatility (standard deviation), ξ is a random number generated by using the standard normal distribution N(0,1), and q is the accident frequency.

Factor $\xi\left[1+\sum_{q=0}^{i}\left(e^{-\lambda}\frac{\lambda^{q}}{q!}\right)\right]$ represents the Wiener process that can affect the volatility σ (figure 4).

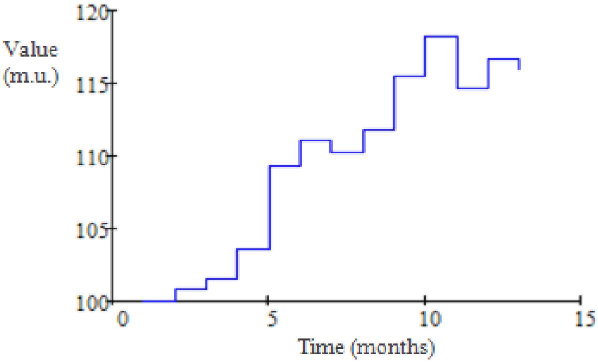

Fig. 4 The evolution of acquisition, repair and upgrade costs

This process was modeled using a Poisson distribution (specific for rare events), and the sum represent the discretization of the integral that characterizes continuous time processes.

$$\eta = 1+\mu \qquad (8)$$

To assess the benefits (B) expressed by reducing the number of accidents due to investment in safety, we propose a model where, at the appearance of a jump, benefit changes with good operating system level probability p. The benefit equation is:

$$B_{t+1}=B_{t}\left[(1+p)+\sigma_{1}\cdot\xi\left[1+\sum_{q=0}^{i}\left(e^{-\lambda}\frac{\lambda^{q}}{q!}\right)\right]\right] \qquad (9)$$

In the benefit equation (9), σ is the volatility (in conjunction with human errors) and ξ is a random number generated using the standard normal distribution N(0,1).

Annual probability of accidents at the system level depends on the connecting elements and is determined by the mean time before failure (MTBF) rate.

The outcome of safety investment project is calculated based on the cumulative benefits and costs using Mathcad program (figure 5). The critical probability of producing accident (that involves total review of the resilience) is associated with time τ, when the benefits outweigh the costs.

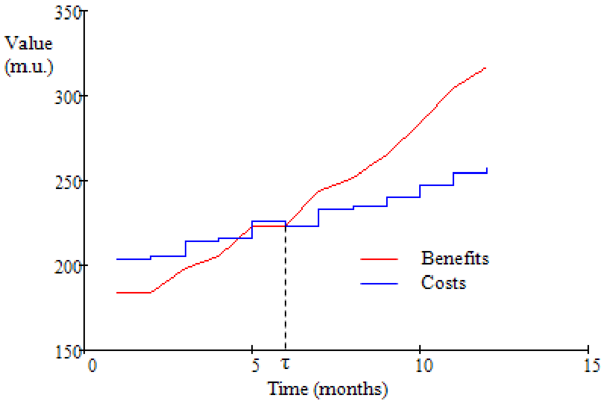

Fig. 5 The outcome of safety investment project

Numerical computation reveals investment opportunity in safety for different values of yield and volatility. Results are highly sensitive to the asymmetry of jumps size and the system architecture. Neglecting jump risk can lead to significant underestimation of the real value of investment opportunities, with negative consequences for decision-making.

CONCLUSIONS

The model was implemented as a simple, fast and efficient tool using Mathcad program, a tool in which data can be simulated by concrete elements of the application.

The advantages of the model concern the introduction of flexibility ingredient essential in decision making. It also incorporates market mechanisms that allow resumption of study in a unique way for this type of applications.

The development of a model that captures the impact of fluctuations resources (technological shocks and human error) in projects safety investment (Wiener process modeled using Poisson distribution) aims to identify management solutions that increase the value of the investment opportunity in high-tech systems.

The limits of the model are related to capturing the interdependencies and interconnections between the technical and socio-human subsystems highlighted by the higher probability of producing the accident at the system level compared to the failure rate at an indispensable functioning component level.

BIBLIOGRAPHY

1. Haimes, Y. Y. Toward a holistic approach to risk management (Guest Editorial), *Risk Analysis* 9 (1989), 147-149.

2. Covey, S. R. *The Seven Habits of Highly Effective People*. New York: Simon and Schuster (1989).

3. Sage, A. P. *Methodology for Large Scale Systems*, New York: McGraw-Hill (1977).

4. Blauberg, I. V., Sadovsky, V. N., Yudin, E.G. *Systems Theory: Philosophical and Methodological Problems*, New York: Progress Publishers (1977).

5. Haimes, Y. Y. *Hierarchical holographic modeling*, IEEE Transactions on Systems, Man, and Cybernetics. 11(1981), 606-617.

6. Burlacu, G., Dăneţ, N., Bandrabur, C., Duminică, T. *Fiabilitatea, mentenabilitate şi disponibilitatea sistemelor tehnice*. Bucureşti: Matrix Rom (2005).

7. Reason , J. *Managing the Risks of Organizational Accidents*. London: Ashgate (1996).

8. Johnson , W.G. *MORT Safety Assurance System*. New York: Marcel Dekker (1980).

9. Rasmussen , J., Svedung, I. *Proactive Risk Management in a Dynamic Society*. Stockholm: Swedish Rescue Services Agency (2000).

10. Ezell, B.C., Bennett, S.P., Von Winterfedt, D., Sokolowski, J., Collins, A.J. Probabilistic Risk Analysis and Terrorism Risk. *Risk Analysis*, vol. 30, nr. 4 (2010), 575-589.

11. Cirka, C.C., Corrigall, E. A. Expanding possibilities through metaphor: Breaking biases to improve crisis management. *Journal of Management Education*, 34 (2010), 303-323.

12. Rasmussen, J. Human error and the problem of causality in analysis of accidents. In *Human Factors in Hazardous Situations.* Oxford: Clarendon Press (1990).

13. Dhillon, B.S. *Safety and Human Error in Engineering Systems*. CRC Press (2012).

14. Dhillon, B.S. *Human Reliability, Error, and Human Factors in Engineering Maintenance: with Reference to Aviation and Power Generation*. CRC Press (2009).

15. Cioacă, C., Boşcoianu, M., Model of Assessing the Impact of Rare Events in Aviation Security Investments Projects. *Applied Mechanics and Materials*, Vol. 555 (2014), 11-17.