IETI Transactions on Engineering Research and Practice
http://ieti.net/TERP/

2018, Volume 2, Issue 1, 17-25, DOI 10.6723/TERP.201806_2(1).0003

THE IMPACT OF VARIABILITY OF FAILURE PROBABILITIES ON THE RELIABILITY OF MULTIPLE SAFETY CONTROLS

Antonis Targoutzidis
26th October, ELINYAE, Thessaloniki, Greece
targoutzidis@elinyae.gr

Abstract Although most failure probabilities vary in time, the effects of this variability have not been sufficiently discussed in literature. In this paper, it is attempted to assess the impact of the variable failure probability of degrading safety controls, investigating whether point estimates (mean values) of failure probability are adequate proxies. Moreover, the time-related effects of corrective intervention are also examined i.e. whether the synchronization of replacements of safety controls affects the overall reliability. The assessment takes place through Monte Carlo simulation and ANOVA in three simple systems of degrading components: one single safety control, two identical safety controls in series and two parallel safety controls. Point estimates appear to be an adequate proxy only for one single safety control of variable failure probability. Particularly in parallel safety controls, differences are large enough to reject this hypothesis. Moreover, the effect of synchronization of the replacements of the two safety controls appears to have a large impact, particularly for parallel systems, where failure probability is minimized for phase difference of 50% of lifecycle between replacements.

Keywords: Replacement; variable failure probability; parallel components; degrading systems.

1. INTRODUCTION

Although it is widely accepted that most real-world systems are subject to dynamic influences and, hence, variable failure probabilities, the effect of the variability of failure probabilities has not been sufficiently discussed in literature. In this paper it is attempted to investigate a simple case of variable failure probability and the extent to which its results differ from those of an equivalent stable probability.

Like all material systems, safety controls are subject to tear and wear, which gradually reduces their reliability, i.e. increases their failure probability [1-2]. Inevitably, this leads to maintenance or replacement of the safety controls to bring back failure probability to acceptably low levels. The result is a dynamic pattern of failure probability, with a variability that increases with the level of complexity of the system [3].

Although the variation of failure probability during the lifecycle of a safety control can be large, it is very difficult to monitor its (periodic or not) evolution and use it for decision making, especially in complex systems with many and different safety controls that interact. This situation is usually dealt with the use of a point estimate of reliability (i.e. the desired maximum cumulative failure probability) for every safety control, and by adjusting the replacement period in order to remain under this threshold.

2018, Volume 2, Issue 1, 17-25, DOI 10.6723/TERP.201806_2(1).0003

However, this same cumulative point estimate can be obtained by different shapes of failure probability density function (constant included), so that important information may be overlooked (e.g. see [4]). This can be particularly important in more complex systems with various safety controls, as the synthesis of their dynamic nature can lead to serious differentiations [5]. Especially for complex systems, the impact of time-dependent failure probability has been an issue for various approaches, such as the asynchronous evolution [6-7], resilience [8], etc.

A characteristic insight on the static model of Reason [9] is given in [10] as a dynamic "Swiss Cheese" whose holes open and close and may coincide in certain "time-windows".

The pattern of increasing failure probability that is steeply minimized after a replacement or maintenance has been presented as a "saw tooth" curve (Figure 1) in previous works [11]. This type of curve represents any "bell-shape" type of failure probability distribution (Weibul, Gamma, Normal, etc.), which is the general case for failure probability of degrading safety controls.

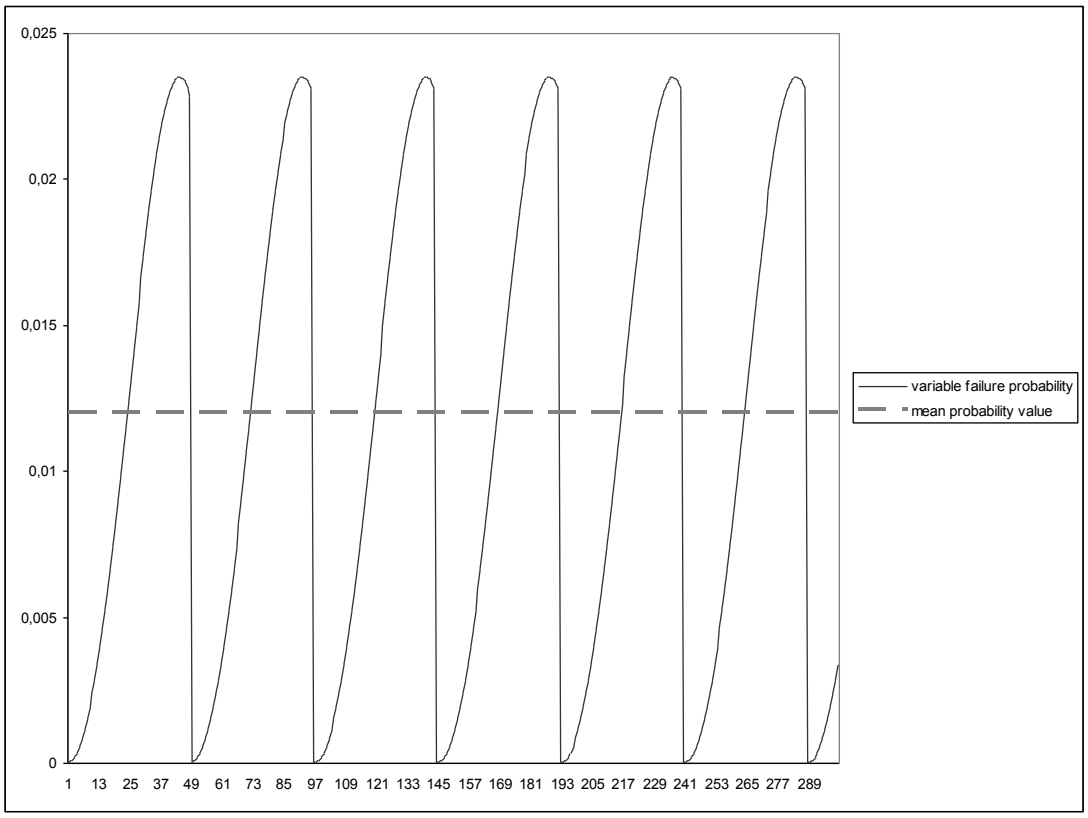

Figure 1. The "saw-tooth" pattern for failure probability.

Especially for complex systems, the co-existence or interaction of many "saw-tooth" curves produces a total failure probability curve of a "spectrum-like" shape with sharp peaks, which illustrates the "dynamic Swiss Cheese" mode. However, whether this complex failure probability can be represented by constant probability estimates has not been sufficiently examined.

2018, Volume 2, Issue 1, 17-25, DOI 10.6723/TERP.201806_2(1).0003

Despite criticism on their true independency [12] the use of parallel (redundant) safety controls is a common practice to increase the reliability of a system. However, as it is also evident in the simulation of this paper, the important increase of reliability that they provide, comes with a greater dependency on time variability of failure probability. A different replacement policy (i.e. whether replacement of both controls takes time simultaneously or whether there is a "phase difference" between the replacements and subsequently between the failure probability patterns of the different safety controls) could have a large impact in the overall failure probability of the system.

This paper aims to investigate the impact of this time-related variability and the extent to which point estimates of probability are efficient as proxies, i.e. whether they can adequately predict the number of failures. Such an investigation can only take place through simulation; therefore Monte Carlo simulation has been applied in three different versions of a simple system:

a) one safety control, b) two identical safety controls in series and c) two identical parallel safety controls. Versions with two safety controls are examined in cases of various replacement schedules.

In all versions, the results are compared to those expected by point estimates of failure probability, in order to assess the adequacy of their point estimates. This assessment takes place both in statistical (hypothesis testing) and qualitative way.

2. METHODOLOGY

To present the impact more evidently, the versions and cases were chosen to be as simple as possible. The basic unit is a safety control whose failure probability follows a Weibul distribution with a beta factor of 3 and an eta (lifecycle) factor of 50. Replacement takes place every 48 periods (Figure 1).

Three versions were examined:

a) one safety control. P=P1

b) two identical independent safety controls in series: P = P1 U P2 = P1+P2- P1•P2

c) two identical independent parallel safety controls: P = P1 ∩ P2 = P1•P2

Versions b and c are examined both in the case of simultaneous replacement and 50% phase difference in replacement (24 periods between the replacement of the first and the second control).

To obtain a better sample (particularly for the simulation), testing period was set to 30000 periods.

$$P_1 = \frac{b}{n}\left(\frac{x-r}{n}\right)^{b-1} e^{-\left(\frac{x-r}{n}\right)^{b}} \quad (1)$$

IETI Transactions on Engineering Research and Practice
http://ieti.net/TERP/

2018, Volume 2, Issue 1, 17-25, DOI 10.6723/TERP.201806_2(1).0003

$$P_2 = \frac{b}{n}\left(\frac{x+ö-r}{n}\right)^{b-1} e^{-\left(\frac{x+ö-r}{n}\right)^b} \quad (2)$$

r: replacement term = $s \cdot trunc\left(\frac{x+ö}{s}\right)$

x: period = 1-30000

b: beta factor = 3

n: eta factor = 50

φ: phase difference in replacement = 0 or 24

s: number of periods per replacement = 48

The structure is shown in Table 1.

Table 1. Versions examined in the model.

Period	**P_1**	**P_2**	**$P_1 \cap P_2$**	**$P_1 \cup P_2$**
1	$P_{1,1}$	$P_{2,1}$	$P_{1,1}+P_{2,1}-P_{1,1}\cdot P_{2,1}$	$P_{1,1}\cdot P_{2,1}$
2	$P_{1,2}$	$P_{2,2}$	$P_{1,2}+P_{2,2}-P_{1,2}\cdot P_{2,2}$	$P_{1,2}\cdot P_{2,2}$
...	...			
30000	$P_{1,30000}$	$P_{2,30000}$	$P_{1,30000}+P_{2,30000}-P_{1,30000}\cdot P_{2,30000}$	$P_{2,30000}\cdot P_{2,30000}$

The aim of this paper is to investigate the theoretical impact of dynamic probabilities, and therefore the assumptions for the simulation were kept as simple as possible. A failure occurs when one (in cases a and b) or both (in case c) safety controls fail. In case of failure of any safety control, to avoid the effects of real-world situations (that would affect the theoretical investigation), this failure was assumed to be immediately detected and replacement would not affect the probability curve. Otherwise, the effects of late detection and replacement or a new failure probability curve could be dominant to the final results.

The minimum number of trials required for an adequate Monte Carlo simulation is 100/P [13], which is 8337 trials for the certain safety control. The 30000 period interval was replicated 8337 times and the events were tested by ANOVA and mean value hypothesis testing for all versions and cases.

IETI Transactions on Engineering Research and Practice
http://ieti.net/TERP/

2018, Volume 2, Issue 1, 17-25, DOI 10.6723/TERP.201806_2(1).0003

Table 2. Simulation structure.

Period	single		$P_1 \cap P_2$			$P_1 \cup P_2$		
	variable	stable	0%	50%	stable	0%	50%	stable
1	$P_{1,1}$	$\overline{P_1} \cdot \overline{P_2}$	$P_{1,1} \cdot P_{2,1}$	$P_{1,2} \cdot P_{2,2}$	$\overline{P_1} \cdot \overline{P_2}$	$P_{1,2} \cdot P_{2,2}$	$P_{1,2} \cdot P_{2,2}$	$\overline{P_1} \cdot \overline{P_2}$
2	$P_{1,2} \cdot P_{2,2}$	$\overline{P_1} \cdot \overline{P_2}$	$P_{1,2} \cdot P_{2,2}$	$P_{1,2} \cdot P_{2,2}$	$\overline{P_1} \cdot \overline{P_2}$	$P_{1,2} \cdot P_{2,2}$	$P_{1,2} \cdot P_{2,2}$	$\overline{P_1} \cdot \overline{P_2}$
...	...	...	...	...	...	...	...	...
30000	$P_{1,30000}$	$\overline{P_1} \cdot \overline{P_2}$	$P_{1,30000} \cdot P_{2,30000}$	$P_{1,30000} \cdot P_{2,30000}$	$\overline{P_1} \cdot \overline{P_2}$	$P_{1,30000} \cdot P_{2,30000}$	$P_{1,30000} \cdot P_{2,30000}$	$\overline{P_1} \cdot \overline{P_2}$

3. RESULTS

In the version of one single measure, the mean probability value appears to be an adequate proxy. With a stable probability equal to the mean value of the variable one, 73.36 incidents would be expected in the 30000 periods, compared to 73.33 of the variable ("saw-tooth") probability density function (pdf). Results are presented in Table 3.

Table 3. Comparison of point estimate and variable failure probability for a single control measure.

ANOVA	Mean		SST	DoFT	MST	SSE	DoFE	MSE	F
Single variable	0.00244	0.00244	$5.39\ 10^{-9}$	1	$5.39\ 10^{-9}$	0.0015	16670	$8.86\ 10^{-8}$	**0.06**

The critical value for α=0.05 level of significance is 3.84 and therefore the null hypothesis for equal mean values is accepted.

Mean values are also close enough in the version of two safety controls in series. A stable probability equal to the sum minus the product of mean values of the safety controls would predict 146.71 incidents in the 30000 periods examined, compared to 146.93 incidents for the case of simultaneous replacement and 146.98 incidents for the case of 50% phase difference. Results are presented in Table 4.

Table 4. Comparison of point estimate and variable failure probability for two control measures in series for simultaneous replacement and 50% phase difference.

ANOVA	Mean		SST	DoFT	MST	SSE	DoFE	MSE	F
Series 0%	0.0049	0.0049	$3.7\ 10^{-7}$	2	$1.8\ 10^{-7}$	0.004	25005	$1.6\ 10^{-7}$	1.14
Series 50%	0.0049								
Series stable	0.0049								

The critical value for α=0.05 level of significance is 3.00 and therefore the null hypothesis for equal mean values is accepted.

2018, Volume 2, Issue 1, 17-25, DOI 10.6723/TERP.201806_2(1).0003

The differences are large in the version of parallel safety controls. A stable probability equal to the product of mean values of the safety controls would predict 0.18 events in the 30000 periods examined, compared to 0.29 events for the case of simultaneous replacement and 0.13 events for the case of 50% phase difference. Results are presented in Table 5.

Table 5. Comparison of point estimate and variable failure probability for two parallel control measures for simultaneous replacement and 50% phase difference.

ANOVA	Mean		SST	DoFT	MST	SSE	DoFE	MSE	F
Parallel 0%	$9.6\ 10^{-6}$	$6.64\ 10^{-6}$	$1.25\ 10^{-7}$	2	$6.29\ 10^{-8}$	$5.5\ 10^{-6}$	25005	$2.198\ 10^{-10}$	286
Parallel 50%	$4.3\ 10^{-6}$								
Parallel stable	$6\ 10^{-6}$								

The critical value for α=0.05 level of significance is 3.00. The difference is large and (as expected) statistically significant, so that the null hypothesis of equal mean values is rejected for every couple of cases.

4. DISCUSSION

According to the findings of this simulation, a point estimate is an adequate proxy both in the cases of a single safety control and the case of two identical safety controls in series. In the version of parallel safety controls, the case is clear (statistically and qualitatively) that even the true mean value as a point estimate is not an adequate proxy. Although the mean probability value is the same, the number of failure events is significantly different.

This is an expected result of linearity, which only exists in version a. In the case of safety control in series, the non linear factor (P1•P2) is smaller compared to the other terms (P1, P2), so that the impact is small. However, this is the only term of version c, which makes its impact much larger.

In other words, adding variable probabilities does not lead to significant errors, which is not also the case for multiplying them. In the latter case, calculations based on point estimates of reliability of the components are far from being accurate.

Another parameter examined in versions b and c is the synchronization of replacements. This is also an effect of linearity and depends on the term P1•P2. This term has a negative sign in version b, which makes simultaneous replacement a positive influence for safety, so that with this replacement strategy, less incidents are expected.

However, in the case of parallel safety controls, this term has a positive sign, which makes simultaneous replacement a negative influence for safety, as much more incidents are expected with this replacement strategy.

This is evident in the combined graph of Figure 2, where simultaneous replacement gives much higher values of total failure probability.

IETI Transactions on Engineering Research and Practice
http://ieti.net/TERP/

2018, Volume 2, Issue 1, 17-25, DOI 10.6723/TERP.201806_2(1).0003

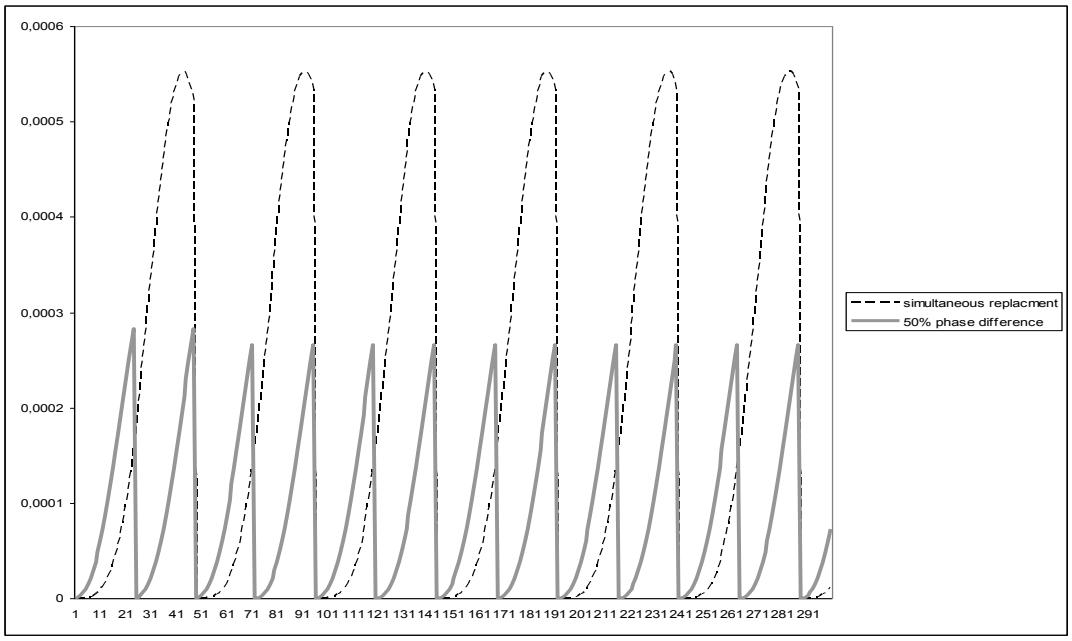

Figure 2. Comparison of probability density function for simultaneous replacement and phase difference 50% of the lifecycle.

The cases of 0% and 50% that were examined are the two extreme values, as the product of mean values of the components varies upwards or downwards from the total mean value of the system according to this phase difference, as shown in Figure 3.

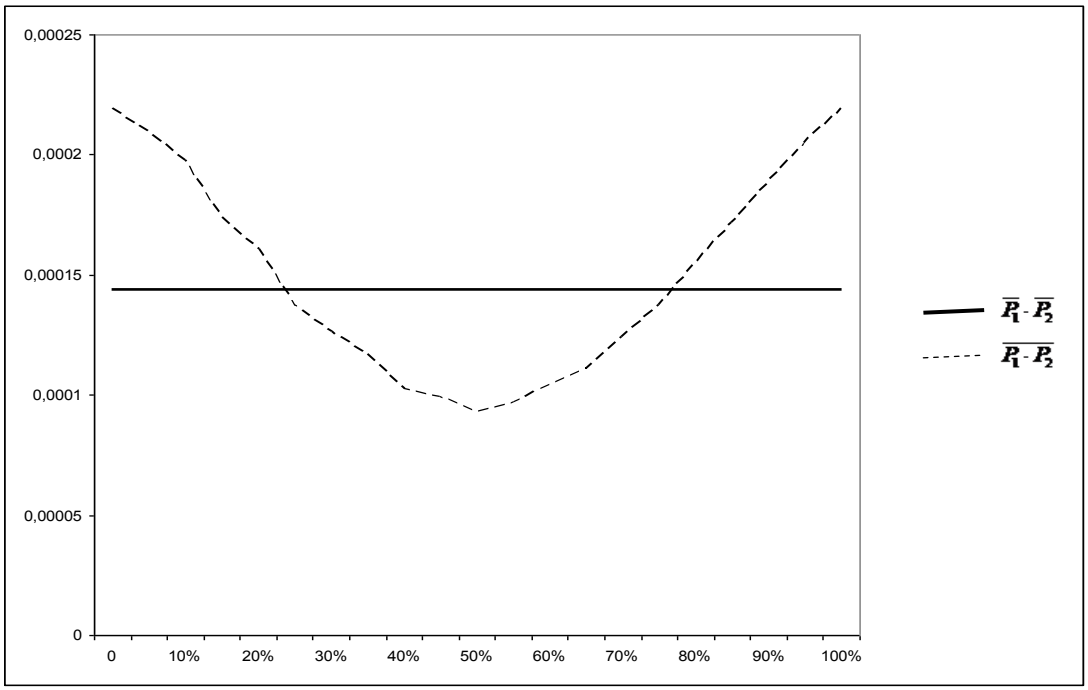

Figure 3: Mean failure probability value of the system for various values of phase difference compared to the product of mean values of the components

2018, Volume 2, Issue 1, 17-25, DOI 10.6723/TERP.201806_2(1).0003

Thus, there are two main conclusions for reliability analysis in the general case of degrading reliability:

•Calculation based on point estimates of the components of a system are not a sufficient proxy for its reliability, especially when parallel components are involved.
•Phase difference in the replacement strategy of identical safety controls can reduce reliability in components in series and can increase reliability in cases of parallel systems.

Since the cost of replacements (cost of component plus cost of stoppage) is the main disadvantage of a non-simultaneous replacement strategy, such a strategy is absolutely meaningless in the case of components in series. In the case of parallel components, it is mainly feasible only for 50% phase difference, as in all other cases except from simultaneous replacement, the number (and cost) of replacements will be the same but the reliability will be smaller. Such a replacement strategy of 50% phase difference, is a better option than simultaneous replacement only if the improved reliability that it provides outscores the double time of stoppages for replacement; therefore such a choice depends on the situation (i.e. the cost of failure compared to the cost of replacement).

Of course, there should be no general conclusions, as the results depend on the situation. Moreover, there are further phenomena (e.g. common cause failures) for identical systems that can also affect their reliability. The systems examined here were simple in order to present the theoretical effects. However, in real-world systems, many safety controls of variable failure probability co-exist or interact, potentially with also variable input (e.g. pressure, temperature, etc.) Moreover, replacement of a safety control after a failure could either be delayed (e.g. due to poor detection) or take place with a new safety control, which disturbs the synchronization of lifecycles.

These facts make the situation much more complex with non-periodic patterns and resonance phenomena that can cause large variation in the overall failure probability. Especially for these cases, linear (and particularly non-linear) combinations of point estimates of components' probabilities can lead to significant errors, particularly for parallel safety controls.

5. CONCLUSIONS

In this paper it was attempted to investigate the effect of time variability of failure probability of degrading safety controls. More specifically, it was attempted to assess the effect of the synchronization of replacements, as well as the extent to which point estimates of failure probability are adequate as proxies.

The main conclusions are:

•Point estimates of failure probability are adequate estimates only in cases of single measures or safety controls in series; in cases of parallel systems the differences are significant.

•The synchronization of replacements may have a large impact, particularly in parallel systems. Failure probability is maximum for simultaneous replacement and minimum for a phase difference of 50% of lifecycle. The results are opposite and less important for safety controls in series.

2018, Volume 2, Issue 1, 17-25, DOI 10.6723/TERP.201806_2(1).0003

The selection of the replacement pattern is an issue of cost and required reliability and it is situation-related, so that no general conclusions are feasible. However, a non-simultaneous replacement strategy of identical safety controls is meaningful only in parallel systems and a 50% phase difference.

Nevertheless, the main conclusion of this analysis is that the variability of a failure probability has an effect of its own (i.e. it differs compared to the results of a constant one - e.g. equal to its mean) in any non linear system and this phenomenon needs to be further investigated.

References

[1] Mol T., 2002, An Accident Theory that Ties Safety and Productivity Together, *Occupational Hazards. EHS Today*. http://www.ehstoday.com/mag/ehs_imp_35910.
[2] Montoro-Cazorla D., and Peréz-Ocón R., 2006, A Deteriorating Two-System with Two Repair Modes and Sojourn Times Phase-Type Distributed, *Reliability Engineering and System Safety*, 91, pp.1-9.
[3] Perrow C., 1984, *Normal Accidents, Living with High-Risk Technologies,* N.Y. Basic Books, New York.
[4] Cox LA Jr., 2009, Some Limitations of Frequency as a Component of Risk: An Expository Note, *Risk Analysis*, 29(2), pp.171-5.
[5] Vernez D., Buchs D., Pierrehumbert G., and Besrour A., 2004, MORM – A Petri Net Based Model for Assessing OH&S Risks in Industrial Processes: Modeling Qualitative Aspects, *Risk Analysis*, 24(6), pp.1719-35.
[6] Leplat J., 1984, Occupational accident research and systems approach, *Journal of Occupational Accidents*, 6, pp. 77–89.
[7] Levenson N., 2004, A New Accident Model for Engineering Safer Systems, *Safety Science,* 42, pp. 237-270.
[8] Haimes Y. Y., 2009, On the Definition of Resilience in Systems, *Risk Analysis*, 29(4), pp. 498-501.
[9] Reason J. T., 1990, *Human Error,* Cambridge University Press, Cambridge.
[10] Körvers P. M. W., and Sonnemans P. J. M., 2008, Accidents: A discrepancy between indicators and facts, *Safety Science,* 46, pp.1067-1077.
[11] Targoutzidis A., and Antonopoulou L., 2006, Interference Phenomena in Temporal Evolution of Accident Probability in Workplaces, *Risk Analysis,* 26(3), pp. 671-682.
[12] Paté-Cornell M. E., Dillon R. L., and Guikema S. D., 2004, On the Limitations of Redundancies in the Improvement of System Reliability, *Risk Analysis*, 24(6), pp. 1423-36.
[13] Bomel Ltd., 2001, Probabilistic Methods: Uses and Abuses in Structural Integrity, HSE Contract Research Report 398/2001. http://www.hse.gov.uk/research/crr_pdf/2001/crr01398.pdf.