

**THE RISK ASSOCIATED WITH EMPLOYEES' ERRORS  
IN ENTERPRISES WITH CRITICAL INFRASTRUCTURE DEFINED  
IN EXECUTIVES TERMS**

**Olton I., Glowacki D.\***

**Abstract:** No in-depth research in the area of risk management of the human factor in organizational processes (in particular operational ones) is without doubt an important issue in effective risk management, particularly in units managed with critical infrastructure. The absence of systemic solutions, models, algorithms for predicting employees' risky behavior causes management's ignorance, not recognizing problems, a lack of forward-looking perspective and focus on nothing but the current issues of the organization. This article attempts to explain the need for dynamic assessment of the risks of human error in management terms because only such assessment can increase resilience to crises in companies with critical infrastructure. In the following study, the concept of 'the risk of a human factor' will be used interchangeably with the term 'the risks associated with employees' errors' that are generated by behavioral risk and the risk of latent skills gaps.

**Key words:** critical infrastructure, the risk of human factors, the risk of human error

**Introduction**

The risk described in the literature is treated either as a general phenomenon occurring in business management or refers to a specific risk, i.e. its particular category, e.g. a regulatory risk, a currency risk, a training risk, etc. Relatively little is written about the risks in general, also taking into account the human factor in organization. Although the staff is a source of innovation and the key to sustainable development of the company, they carry the greatest risks at the same time (Iwu and Benedict, 2013). In the literature on the subject, there is almost unanimous agreement that the critical (weak) parts of entrepreneurial systems are related to the human factor, i.e. to their users (Frangopoulos et al., 2013) who have individual characteristics in terms of skills. Still, it is impossible to classify a lack of skills easily. Often, human errors are equated with machine failures by analogy. Besides, it is believed that all kinds of behavior are correct in a given situation. The problem is also that some of the undesirable effects may influence only certain parts of the system (Myszewski, 2012). Moreover, the risk lies in the employee's overall health condition (e.g. discomfort, anger, tension, forgetfulness, recklessness, negligence, boredom, a lack of sleep and other states). Thus, it is evident that the human availability is uncertain and thus the risk is natural. However, there is a lack of specific tools which allow to manage such an important risk in a systemic manner with its complexity and variability being considered.

---

\* **Izabela Olton, PhD**, Czestochowa University of Technology, **Dominik Glowacki, PhD**,  
Warsaw University of Technology

✉corresponding author: [iolton@bud.pcz.czest.pl](mailto:iolton@bud.pcz.czest.pl)

✉corresponding author: [glowacki\\_dominik@yahoo.pl](mailto:glowacki_dominik@yahoo.pl)

The following study attempts to explain the need for dynamic assessment of the risks of human error in management terms in companies with critical infrastructure. Critical infrastructure is the term used in reference to the resources which are essential for the functioning of society and the economy; in accordance with the Act on crisis management, critical infrastructure shall be understood as "systems and functionally related objects belonging to them, such as building structures, equipment, installations, services that are crucial to the security of the state and its citizens, and services ensuring the smooth functioning of the public administration, the institutions and entrepreneurs".

### **The nature of risk of the human factor**

Risk is a dynamic and complex issue because it may have different values in different configurations. Apart from that, there are important interconnections between different types of risk. For example, the personal (behavioral) risk is closely related to other types of risk, including technological risk which concerns, in particular, the great critical public infrastructure, such as power, gas, water, sewage and telecommunications, as well as the so-called high-risk industries (nuclear power plants, chemical plants). Employees (human factor) and material resources "work together" within the defined limits of the system. In other words, the efficiency of the system (organization) depends largely on employees (risk management associated with them) (Marescaux et al., 2013).

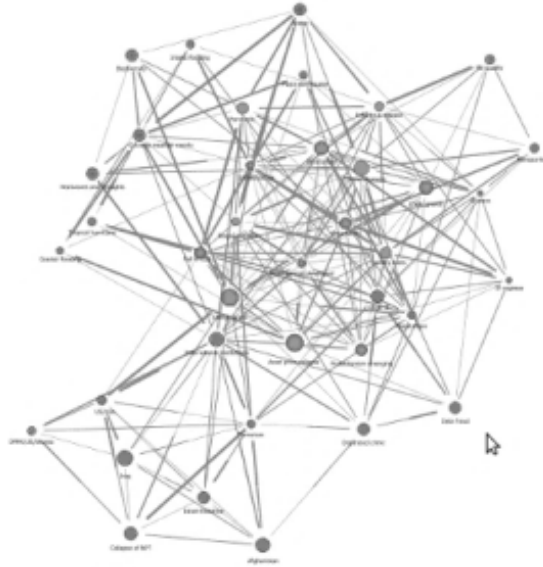
While analyzing the literature, it is clear that the risk of the human factor in a company is not investigated in a comprehensive manner (systemic). The classic approach to the risks associated with the human factor in the company (the risk of human capital, personal risk, occupational risk), recorded and analyzed fragmentarily, does not allow to capture its specificity, that is, the variability and complexity. Furthermore, the systemic approach to the risks associated with employee's participation in operational processes of a company is undertaken in the literature of the subject mainly from the point of view of job safety management. Generally, the risk of human participation in the functional processes of a company in both the U.S. and Europe is narrowed to the risk involved in job security or reduced to one category (e.g. the key personnel risk, the risk of human capital). There is no risk assessment system of the human factor in the dynamic approach, also in conjunction with the risk assessment of processes supported and implemented by the staff. Only such a context of the assessment can provide the basis for more predictability in the area of enterprise risk management (Lipka, 2002). Reducing the risk of human factor only to the next category narrows significantly a research perspective. It does not match the reality and reduces the risk factor only to assessment of human risk.

### Practical perspective of risk perception

The risk is present in all spheres of human activity at the time when people are not able to control or to predict accurately the future. The division into risk categories makes it easier to describe the cause-effect relationship, with a clear distinction between causes and effects, according to fixed and repeatable elements. This allows one to concentrate on the search for causes (Navare, 2003). However, there is one question to be asked. Does the identification and codification of the maximum amount of risks is helpful in the description of the cause-effect relationship of one or many named items? In many cases based on life experience, one should get to know the whole structure/the tree of cause and effect. What is more, one critical link should be chosen and the risk identification, even if there is such, is not sufficient.

A major threat may be a lack of a balance between identified types of risks that occur with the professional methods / engineering methods at the stage of assessing and measuring its kinds (Kierner, 2010). Therefore, the aim is not to identify the greatest number of the risks. The aim is to discover its previously unknown kinds and dependences.

In conclusion, the analysis of the risks associated with employee's participation in organizational processes cannot be limited only to the risk assessment at the workplace or within any accepted category. The network nature of the risk, which is made up by its various types, is presented in the Figure 1.



**Figure 1. Map of risk (The Global Risks Landscape, 2009)**

On the attached diagram, the various points mean categories of risk: strategic risks, business risks, those associated with human participation in the organizational

processes etc. The effectiveness and efficiency of risk management, however, depends on the extent to which all the possible risks the organization is exposed to will be identified. The step to calculate risk is crucial. If it is done in an incorrect or incomplete way, the next steps are subject to increasingly larger system errors. Therefore, the process of identification most often narrows down to risk assessment at the workplace (assessment of risk on a position) or of a profession (occupational risk assessment), whereas serious threats not necessarily relate directly to the position or profession under examination, and, consequently, are omitted (Navare, 2003; Tabor, 2013). Practice also shows that the identification of hazards is often incomplete and never expresses all its aspects. Therefore, there is the need to establish the so-called field of risk tolerance. Other errors in risk assessment are also estimating the probability of occurrence of a harmful event and the size of potential losses on the basis of historical data, i.e. frequency in the past. Uncertainty about estimations leads to the so-called subjective perception of risk by the assessors, which, in turn, can cause catastrophic "human errors" and serious material damage (Myszewski, 2012). However, if the level of risk is not properly assessed and its value is not relative to the current value, it is not possible to make correct management decisions. Also, the practice of writing more threats (just in case) on charts of risk assessment on a position does not lead to actual assessment of risk.

Even the concept of ABZ (Job Safety Analysis, described in more detail in the section: The previous state of knowledge) recognizes the problem of the risk of human factor fragmentarily. ABZ focuses only on the elements related to human work. Although the current update of examined aspects is required, the practice proves that an estimate once accepted is in use over a long period of time and has only a purely formal role. In contrast, the risk is subject to dynamic changes in the operational process. The risk that even a "moment" ago was acceptable, "now" can become unacceptable. In other words, the risk analysis depends on the quality and comprehensiveness of the identification of hazards (Navare, 2003).

### **The risk of human factor viewed from the organizational perspective**

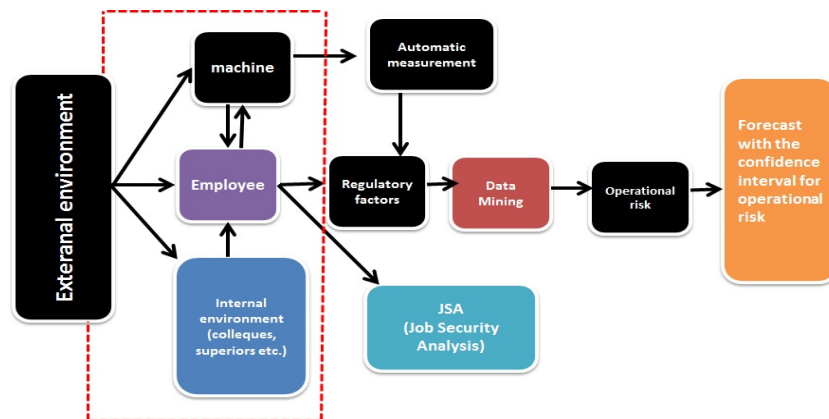
From the point of view of critical infrastructure, the safety of the system and the implementation of processes in a reliable and confident way are priorities. For organizations, however, risks associated with participation of employees in operational processes of the company are important issues. Therefore, knowledge of the factors that generate risk and have the greatest impact on its size is particularly important for companies with critical infrastructure. It should also be noted that the ability to create forecasts on the behavior of employees / symptoms of risky behavior in various situations is very significant in every enterprise (Navare, 2003). It is worth noting that such behavior patterns may be different depending on a context, perception, employee's understanding, as well as his motivation. Moreover, decisions made under conditions of incomplete knowledge can be totally irrelevant to the current situation (Karczewski and Karczewska,

2012). This potentially can lead to negative consequences for employees and organizations.

To manage in the efficient and effective way (on the grounds of the size of risk) the knowledge of risk parameters (potential loss probability) should be regularly updated in connection with aspects relating, inter alia, to employees' behavior / attitudes in the organization (their characteristics - taking into account, inter alia, the dynamic nature), and their competence (McLeod, 2010). Moreover, the system should be as simple as possible, automated, and objectively evaluated for its functioning (a proactive measure). Thus, making the system efficient and effective (reactive indicators) is necessary for its users. As a result, they will have a chance to respond quickly in case of its abnormal functioning (incompatible with assumptions). An analysis and risk assessment should be the reliable sources of information by means of supporting the management of the organization effectively.

### The proposal for the approach to operationalization of risk measurement of the human factor

A modern approach to the issues presented above should rely on creating a set of measurement data in operating conditions of an enterprise so that the model which will use a universal algorithm may be developed. For this purpose, it is necessary to identify systemically potential critical areas related to the participation of employees in operational processes (employees as an integrated part of the organizational environment). The proposal of research model is presented in Figure 2.



--- the area of integration of the employee with the operational process

**Figure 2. Research model**

On the whole, human resources in an enterprise are of a fixed type. Linking them with other resources can contribute to an economic development (minor losses and greater employee satisfaction). The reduction of risk will be achieved by designing

appropriate processes and introduction of appropriate automated control mechanisms on the basis of artificial intelligence. Data for an automated statistical analysis should be collected by the staff that performs functions of the inspectors of company operational processes. These data should also combine psychosocial information about workers with statistical modeling issues.

### Summary

Risk assessment and risk management is an area with great potential for research. It is also the scientific challenge. Whatever the reason might be, the risk of human factors can lead to significant problems for companies. Risk factors are linked to each other, are complex and often coexist. Finding a synthetic measure of quantitative operational risk (the system of its identification) would give an important tool to manage organizational processes in an optimal way with respect to costs. Good results in risk management in the organization are translated into the level of unnecessary losses and on the company's reputation, i.e. on everything what determines the sustainable development of the company (This development is impossible without good risk management). Risk management of the human factor should become an integral and profitable part of business management provided that there is the transition from the development of the objectives in terms of a moral order or a humanitarian obligation to formulating them in terms of efficiency and reliability of processes, including workers who are an integral part of the system. Only on the grounds of such planning, the improvement of an economic performance of enterprises may be carried out.

### References

- Frangopoulos E.D., Eloff M., 2013, Venter L., *Psychosocial risks. Can their effects on the security of information systems really be ignored?* "Information Management & Computer Security", 21(1).
- Iwu Ch., Benedict H., 2013, *Economic recession and investment on human resource information systems (HRIS)*, "Journal of Management Development", 32(4).
- Karczewski J.T., Karczewska K.W., 2012, *Zarządzanie bezpieczeństwem pracy*, ODDK, Gdańsk.
- Karczewski J.T., Karczewska K.W., 2013, *Analiza bezpieczeństwa zadania*, „Przyjaciel przy pracy”, 10.
- Kierner G., 2010, *Bezpieczeństwo osobowe*, [In:] I. Staniec, J. Zawila-Niedźwiecki, *Zarządzanie ryzykiem operacyjnym*, C.H. Beck, Warszawa.
- Lipka A., 2002, *Ryzyko personalne. Szanse i zagrożenia zarządzania zasobami ludzkimi*, Poltext, Warszawa.
- Marescaux E., de Winne S., Sels L., 2013, *HR practices and HRM outcomes: The role of basic need satisfaction*, "Personnel Review", 42(1).
- McLeod J., 2010, *The effectiveness of workplace counseling*, "Counselling and Psychotherapy Research", 10(4).
- Myszewski J.M., 2012, *Management responsibility for human errors*, "The TQM Journal", 24(4).

Navare J., 2003, *Process or Behaviour: Which is the risk and which is to be managed?* "School of Finance and Law", Bournemouth University, Fern Barrow, 29(5/6).

Tabor J., 2013, *Ocena bezpieczeństwa pracy w przetwórstwie przemysłowym na podstawie analizy zagrożeń zawodowych*, [In:] *Innowacje w zarządzaniu i inżynierii produkcji*, (Ed.) Ryszard Knosala, Oficyna Wydaw., Polskiego Towarzystwa Zarządzania Produkcją, Opole.

## RYZIKO ZWIĄZANE Z BŁĘDAMI PRACOWNIKÓW W PRZEDSIĘBIORSTWACH Z INFRASTRUKTURĄ KRYTYCZNĄ ZDEFINIOWANĄ W ZAKRESIE KADRY KIEROWNICZEJ

**Streszczenie:** Brak pogłębionych badań w obszarze zarządzania ryzykiem czynnika ludzkiego w procesach organizacyjnych (w szczególności operacyjnych) jest bez wątpienia istotnym problemem w efektywnym zarządzaniu ryzykiem szczególnie w jednostkach zarządzających infrastrukturą krytyczną. Brak rozwiązań systemowych, modeli, algorytmów predykcji ryzykownych zachowań pracowników powoduje ignorancję kierownictwa, niedostrzeganie problemów, brak myślenia perspektywicznego i koncentrację na bieżących problemach organizacji. W niniejszym artykule podjęto próbę wyjaśnienia konieczności dynamicznej oceny ryzyka, związanego z błędami ludzkimi w ujęciu zarządczym, gdyż tylko taki charakter oceny może zwiększać odporność na zdarzenia kryzysowe w przedsiębiorstwach z infrastrukturą krytyczną. W pracy będzie stosowane pojęcie: ryzyko czynnika ludzkiego zamiennie z pojęciem ryzyka związanego z błędami pracowników, generowanymi przez ryzyko behawioralne i ryzyko utajonych luk kompetencyjnych.

**Słowa kluczowe:** infrastruktura krytyczna, ryzyko czynnika ludzkiego, ryzyko błędów ludzkich

### 风险与雇员的错误相关在企业中与用董事术语定义的重要基础设施

**摘要:** 没有详细研究在的风险管理区域在人的组织操作的过程(特别是)毫无疑问是在风险管理单位有效的管理的一个重要问题特别是在重要基础设施。系统解答, 模型, 预言算法冒险行为管理无知不引起问题, 大混乱, 没有在组织的当前问题的前面认为和焦点。因为评估的仅本质可能增加对危机事件的抵抗在重要基础设施的企业中这篇文章试图说明到动态风险评估, 与在代表团的人的错误有关。工作将可交换地使用与期限: 有错误的人的期限风险的风险雇员引起的, 风险并且冒关于行为的潜在弱点突岩的风险。

**关键字:** 重要基础设施, 风险人为因素人的风险, 人的错误。