Journal of KONBiN 2019
Volume 49, Issue 3
DOI 10.2478/jok-2019-0056

Jacek RYCZYŃSKI
Military University of Land Forces (Akademia Wojsk Lądowych)

HUMAN FACTOR AS A DETERMINANT OF RELIABILITY AND SAFETY OF TECHNICAL SYSTEMS

Czynnik ludzki jako istotny element niezawodności i bezpieczeństwa systemów technicznych

***Abstract**: The article presents the analysis of the state of knowledge about the impact of the human factor on selected aspects of reliability of technical systems based on selected papers delivered at the ESREL 2018 conference, which took place on June 17-22, 2018 in Trondheim, Norway. In the first part, statistical analysis was carried out in the area of thematic and methodological conference papers. Next, the impact of the human factor on the correct functioning of selected technical systems was discussed, using conference papers on the role of man in ensuring an appropriate level of cyber security, the role of expert knowledge in risk assessment, and innovative risk management methods. In summary, challenges for scientists were identified and further research directions in the analysed area.*
Keywords: reliability, technical systems, ESREL, human factor

***Streszczenie:** Artykuł prezentuje analizę stanu wiedzy o wpływie czynnika ludzkiego na wybrane aspekty niezawodności systemów technicznych na podstawie wybranych referatów wygłoszonych na konferencji ESREL 2018, która odbyła się w dniach 17–22 czerwca 2018 r. w Trondheim w Norwegii. W pierwszej części przeprowadzono analizę statystyczną w zakresie obszarów tematycznych i metodologicznych referatów konferencyjnych. Następnie omówiono wpływ czynnika ludzkiego na poprawność funkcjonowania wybranych systemów technicznych posiłkując się referatami konferencyjnymi nt. roli człowieka w zapewnieniu odpowiedniego poziomu bezpieczeństwa cybernetycznego, roli wiedzy eksperckiej w szacowaniu ryzyka czy też nowatorskimi sposobami zarządzania ryzykiem. W podsumowaniu wskazano wyzwania dla naukowców i dalsze kierunki badań w analizowanym obszarze.*
Słowa kluczowe: niezawodność, systemy techniczne, ESREL, czynnik ludzki (HF)

1. Introduction

Many definitions of reliability are used for humans. None of these definitions takes into account specific human characteristics that distinguish him from a technical object, such as subjectivity, resulting from his consciousness. Man realizes his requirements consciously. He can determine the degree of his unreliability, as well as see the consequences of failure to meet these requirements. These features, which determine the unique nature of human reliability, put him in a privileged positioning relation to existing technical systems. Unfortunately, they are also a threat resulting from the fact that too high maturity may exceed the possibilities of human perception.

The development of technology and the increase in the quality of construction materials make modern systems more and more reliable, while human behaviour still strongly affects the failure rate of these systems. This is largely due to the greatest weakness of human nature, which is manifested in the fact that even professionals make mistakes [16]. The statement "to err - means to be human" is very popular [26]. Even the most automated systems are prone to human error. As a result, human error remains a significant risk factor that can have catastrophic consequences in industry. Increased awareness of the need to know the impact of human error, allows engineers to eliminate these errors in built systems, and as a result reduces the risk of failure [3-5,13,15]. To optimize the reliability of the entire system, it is necessary to take into account both the reliability aspects of the equipment and the impact of the human factor in the relevant analyses. The first of these elements, i.e. hardware or software reliability, are aspects well known and analysed in design and manufacturing processes, while human reliability is often overlooked - perhaps due to lack of information (lack of data) in this area. Human reliability can be defined as the ability to perform tasks with a minimal risk of error, under certain conditions and at certain times [19,21,23]. This definition takes into account important aspects of human activity, such as accuracy and speed, and the fact that the quality of this activity depends on the material environment. Human reliability is not optional for understanding the overall system reliability, it is simply essential [19]. Conducting an analysis of the reliability of technical systems without taking into account man as a key element of the system is a very imperfect approach. It is necessary that the influence of the human factor was an integral part of the conducted analysis of the reliability of technical systems. While effective human action can lead to the achievement of assumed goals, ineffective action causes a threat to safety, increases the likelihood of breakdowns and accidents or in extreme cases causes death of a person. Properly conducted reliability analysis

should treat man as a key element of the technical system, and only so conducted, is of great importance for improving the safety of the entire environment [19,22].

To achieve the set goal, it is necessary to take into account three important aspects: awareness of the occurrence of risk, the need to make specific decisions and the correctness of conducting selected activities. The conducted activity should be an effective activity in which the results obtained are in line with the planned goal [17,18]. The decisions regarding most of the actions are subject to the risk of failure. In such situations, it is necessary to search for solutions until results are obtained in line with the intended purpose. This approach determines the use of solutions that must take into account the multi-faceted analysis of the functioning of modern technical systems. The basic purpose of using these solutions is to ensure the safe operation of both the manufacturing processes and the operation of technical facilities [17].

This year's European security conference was focused on solving the problems outlined above and reliability of ESREL technical systems, taking place under the auspices of the European Society for Safety and Reliability (ESRA). The conference was held on June 17-21, 2018, and was held at the Norwegian University of Science and Technology in Trondheim. ESREL is not the only cyclical conference in the field of reliability and security in the world, but it is, next to PSAM (Probabilistic Safety Assessment and Management Conference), the largest conference in terms of the number of participants and presented papers. Its uniqueness is above all many years of experience (28 editions) and a very wide thematic scope, covering most aspects related to risk assessment and reliability and security of technical systems.

2. ESREL 2018 conference topics

The topic of twenty-eighth ESREL was 'Safe Society in a Changing World'. 390 articles were presented (fig. 1), issued in conference proceedings, available for the first time in history in the Open Access system. The conference was attended by representatives of 47 different countries - the group "OTHERS" includes 27 countries, of which one conference paper was submitted. The largest number of speeches were given by representatives of Norway and China. Poland in terms of the number of articles ranked fifth.

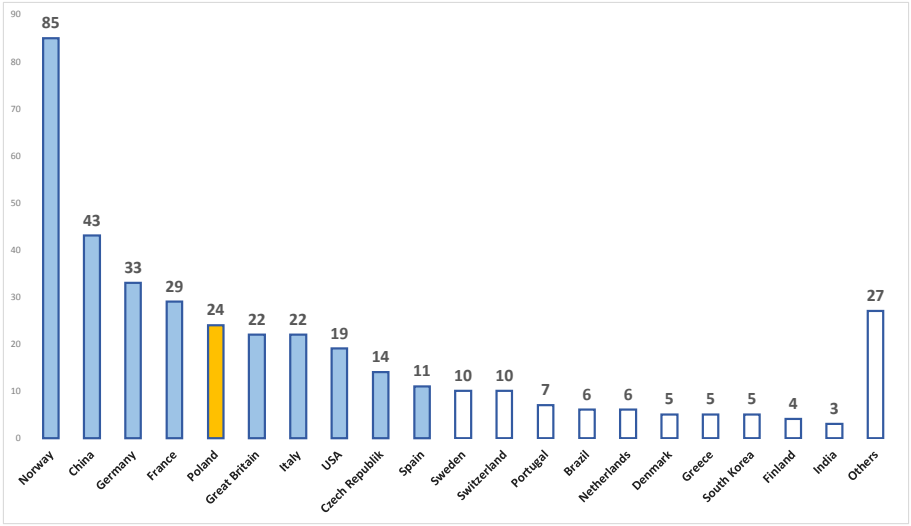


Fig. 1. Number of papers delivered by representatives of individual countries – based on [11]

The conference covered 21 methodological ranges and 21 application areas (fig. 2). It was a forum for presenting and discussing scientific papers on theories, techniques, methods and achievements related to the indicated problems.

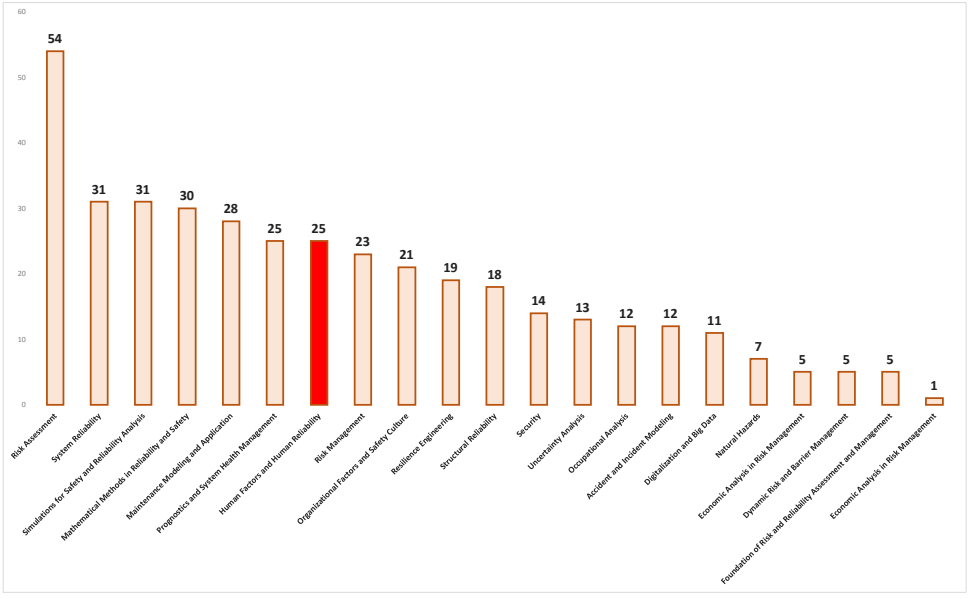


Fig. 2. Number of papers in individual methodological areas and areas of interest – based on [11]

In addition to ESREL's leading areas of the conference, such as risk estimation, risk analysis or mathematical methods and simulation research in the description of risk and safety of technical systems, it is worth paying attention to the growing interest in the area of human factor impact on the functioning of these systems (fig. 3).

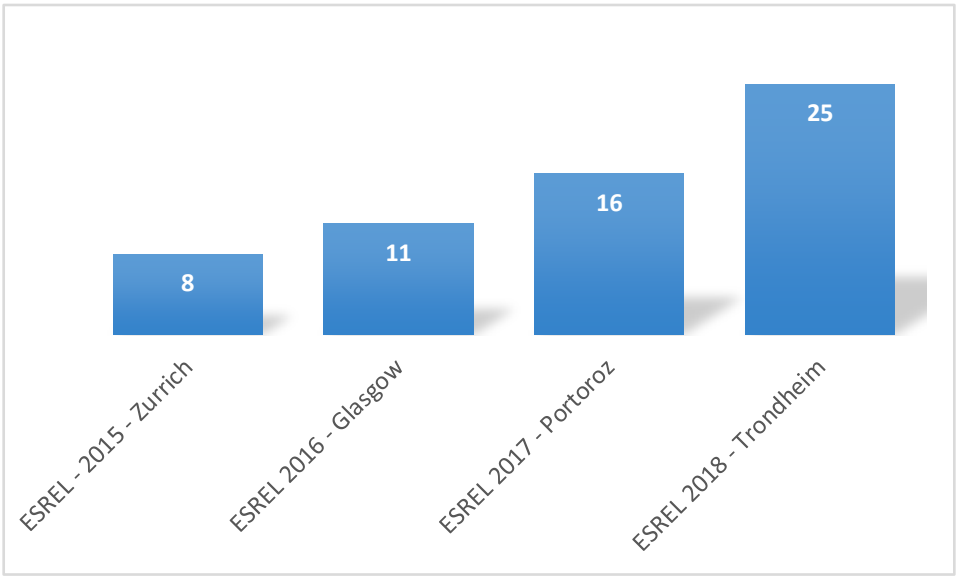


Fig. 3. Number of papers in areas concerning the impact of the human factor (HF) on recent ESREL conferences

From a statistical point of view, this year's ESREL was as follows:

- a total of 101 sessions took place – including 5 thematic special sessions:
  1. Safety and risks in autonomy I.
  2. Safety and risks in autonomy II.
  3. Arctic safety.
  4. Safety and risks in autonomy II.
  5. Risk analysis and safety in standard.
- additionally 2 special sessions in the area of the so-called industrial and workshops:
  1. Major accident collision risk management of dynpos (DP) marine operation.
  2. Industry challenges for railway safety and reliability.
  3. Exhibitors Workshop: Cross – domain safety standards overview with a practical rams lifecycle activities example.

3. The influence of the human factor on the correct functioning of selected technical systems

The analysis of the impact of the human factor on the correct functioning of technical systems consists in determining the extent to which human performance, psychophysical state, general and specialized knowledge and skills as well as interpersonal relationships in the group can negatively affect the system, predicting how often this will happen, and identifying potential consequences, if any [19]. This knowledge is used to optimize system security. Analyses are used to make decisions both in existing and newly designed systems when the risk is high and must be considered at the decision-making level. For existing systems, human factor testing is used to assess problems that need to be improved and to create possible system updates. For systems that have not been built, it is used to evaluate conceptual designs [22].

Analysis of human reliability shows that each technical system has different requirements and affects human reliability differently.

Therefore, it is necessary to use all available tools and methods (the use of systems engineering and behavioural science methods) in the context of assessing the interaction between people and other system components and to enable human error management to optimize system reliability and reduce risk [5]. An excellent reflection of the above statements was the issues raised by keynote speakers in ESREL's plenary lectures. The lectures concerned the following areas [6-9]:

1. the role of man in ensuring an adequate level of cyber security;
2. the role of expert knowledge (human factor) in risk assessment;
3. innovative risk management methods;
4. innovative technologies in obtaining and developing natural resources from deep sea marine deposits.

The common denominator of all these lectures was the influence of man on the functioning of the modern world and the surrounding environment.

The modern world is a ubiquitous technology, and in turn is a closely related problem of security in cyberspace. Therefore, an analysis of the role of man in ensuring an appropriate level of cyber security in large organizations should be carried out [1]. First of all, the question of why cybersecurity is such a significant problem should be answered, and it is on its aspects that the attention of systems managers should focus. According to the Global Risk Report from 2018 [10], cybersecurity was ranked third among the greatest threats to human security after environmental degradation and economic threats [7]. It is not disputed that technology is an element without which the modern environment is not able to

function properly. On the one hand, technology makes life easier, and on the other it is the main source of danger. Man plays a key role in the functioning of every technical system [14]. And he is in many cases the weakest link in any system. "We're starting to think about technology. We combine this technology with security. We think about firewalls, anti-virus programs, passwords, etc. All this is arranged in the form of cyber security! But we tend to forget about one most important key factor - man!" [7] - this is how the problem of human functioning in technical system management was defined. According to research conducted in the USA, 84% of all cyber attacks are caused by human errors or negligence [14]. This data shows that cyber security is a problem that is serious enough to be of interest to the governments of the largest countries in the world. The most serious challenge for system managers seems to be finding a balance between security and privacy, in order to continue to enjoy and use the opportunities offered by technology. It is necessary to understand both processes occurring in every technical system (including technology), but an even more important element is to understand human needs and threats in the network of connections: man - machine - technical system [1,14].

Another aspect of the role of the human factor is the issue of the use of expert knowledge in risk assessment. "It seems impossible to find an analysis of risk and reliability that would not be based on the opinion of experts. This in turn is a fact that is often mentioned as a weakness and a source of doubt as to the reliability of such analyses" [8]. Among the main problems regarding the doubts of expert analyses, five main factors were identified:

- qualifications of the expert conducting the analysis,
- selection of the estimation procedure,
- correctness of the knowledge acquisition process,
- selection of the aggregation method,
- available calibration information (eg. historical knowledge about expert performance).

1. A set of rules of conduct was also formulated, which minimizes the influence of subjectivism on the formulation of expert opinions [8]:
2. A set of opinions from many experts gives more accurate results than the opinion of a single expert (n-heads rule).
3. Mathematical methods of aggregation are generally better than behavioral methods.
4. The quality of opinions can be significantly improved by spreading the complex problem into a number of more elementary problems.

5. There is a noticeable improvement in the results achieved if we use expert consultations at the stage of preliminary definition of the problem and its distribution.

Another aspect of the analysis in the scope of the importance of the human factor's impact on its functioning is the risk management both in the areas normally examined and in areas that are commonly omitted during the analyzes (fig. 4).

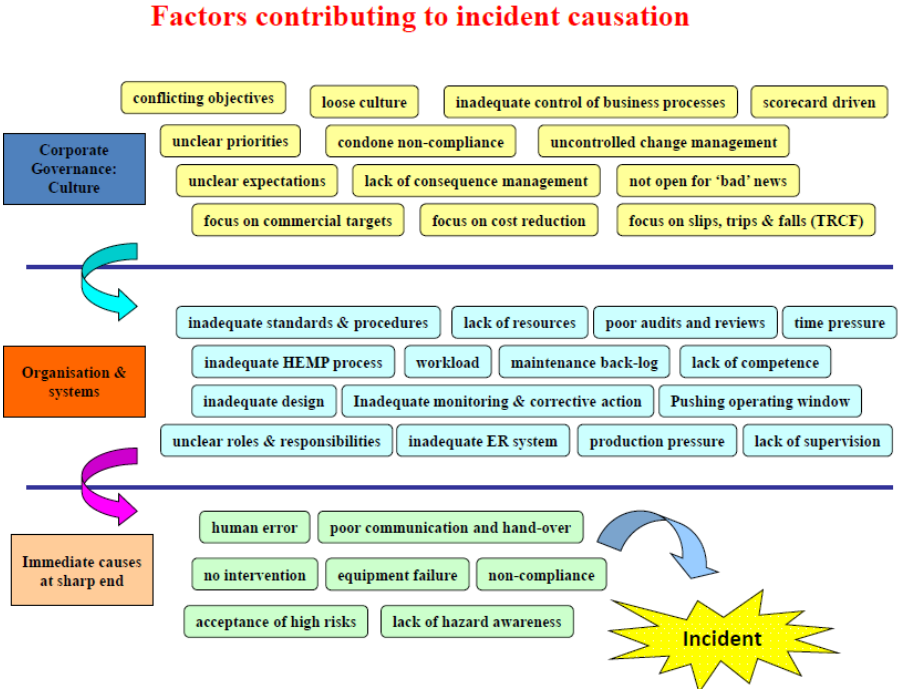


Fig. 4. Groups of factors influencing accidents [6]

The most popular methods of risk management use a rather limited set of reasons or causes that cause them. The majority of potential incidents, around 80%, may be due to linear reasons and deterministic. Of the remaining 20% - 80% of causes can be more and more non-linear, but still deterministic. Overall, this gives 96% [5]. Other potential accidents will have causes that are both non-linear and non-deterministic, i.e. a small set, which is called WEIRD - Wildly Erratic Incidents Resulting in Disaster [12].

All causes of accidents can be included in one of three basic groups:

- type I - defined by simple models covering 80% of all accidents - ordinary personal accidents;

- type II - the next step is 80% rest, in total 96% - complex personal accidents and some organizational accidents;
- type III - the next step is 80% rest, in total 99,2% - complex process and organizational accidents.

For each of the three basic groups has been assigned areas of responsibility that rests at the various levels of managing the organization [6]:

- type I - direct, imposes responsibility on the individual control of an individual employee;
- type II - the management controls the conditions in which we work; the management focuses more on the organization and has less control over the units;
- type III - covers only the area that is within the scope of top management control; the management of this level sets the goals and standards of work we do.

Particular attention in the field of accident should be focused on the aviation industry. In commercial aviation and some other industries, serious accidents are now extremely rare. Simple risk assessment and analysis models often fail to capture how these accidents are caused. The solution to this problem may be a cause and effect set defined as WEIRD. The key to solving rare accidents is understanding the risk space, and the solution is to use the so-called "Three rules" [6]. Accidents are complex events, consisting of over 50 direct and additional factors. Elimination of a single factor can prevent an accident but there can be 49+ other waiting factors, so-called "An Accident Waiting to Happen" [6]. The Three Rule helps develop situational awareness at both the organizational and individual level. Situational awareness tells us how close our organization is to the edge (fig. 5).

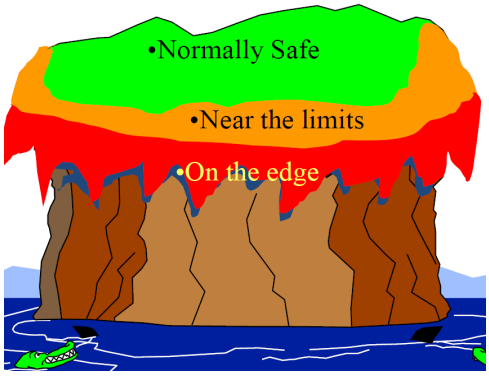


Fig. 4. Safety levels in the "rule of three" [5]

"Rule Three" is based on two boundary levels - green and orange [5]:

- green - keep your actions going;
- orange - proceed with caution;
- red - ruthlessly stop the operation and deal with a comprehensive analysis of the problem,

however, one should remember about the rule: three orange is one red, that is, an absolute stop is required.

Analyzing the impact of human activity on the surrounding systems and conducting the analysis of the impact of human error on changes or degradation of these systems, it is impossible to omit the problems of the natural environment, including the marine environment. One of the biggest threats to the marine environment is the dynamic development of innovative acquisition technologies and the development of deep-sea deposits. Technologies currently used are subject to high risk and are extremely dangerous [9]. This character is a source of new, unique and previously unknown threats. After the Transocean Deepwater Horizon incident and the oil spill in the Gulf of Mexico, the US Department of Homeland Internal Security Office funded the Ocean Energy Safety Institute at Texas A&M University [2,24,25]. At the same time, many other organizations have increased their efforts to solve problems related to management systems and technologies that provide safer and more environmentally friendly operations in the field of ocean energy acquisition [2]. Among the main directions of action in the field of improving the safety of conducting deep-sea mining operations, [9] was indicated:

- development of methods for detecting early tectonic movements,
- introduction of advanced materials to HPHT (high pressure high temperature) conditions,
- corrosion prevention,
- detection of undersea leakage,
- development of high-pressure pressure control equipment,
- development of methods for conducting zonal insulation,
- limiting leaks and mitigating their effects,
- integration of technical, organizational and social aspects of activities - elimination of human errors.

4. Summary

Man has a decisive influence on the safe operation of technical systems, and his activity is crucial from the point of view of the correct functioning of all surrounding systems, including systems as sensitive and complicated as the

natural environment. Analysis of the reliability of the technical system can not neglect the reliability of a human being. Therefore, the issue of human reliability must be an integral part of the analysis of system reliability. Potential human errors increase the level of risk associated with the operation of each system. Despite the generally accepted methods for conducting human reliability analysis, there are great difficulties in accurately assessing the impact of the human factor on the level of safety. Many experts believe that the current methods used are not very detailed and too much simplify the concept of human error, which is why work on new solutions is underway all the time. The article indicates the need to include the subjective character of a human being in these methods, which results from his awareness. Man realizes the tasks in a conscious way, has the ability to assess the changing situation, the ability to act in unusual situations, creativity in solving problems and learning from his and other people's mistakes. However, human nature has its limitations. Therefore, in the analysis of human reliability, it is necessary to pay more attention to the laws governing the psyche and human behaviour, that is taking into account also the psychological aspect. One of the most difficult elements to solve is the formulation of criteria for measurability of human behaviour. Describing the language of human behaviour in crisis situations is undoubtedly the most important challenge for scientists in the near future.

5. References

1. Boy E.: The Handbook of Human-Machine Interaction: A Human-Centered Design Approach. ISBN 9781138075825. CRC Press. 2017.
2. BP, “Deepwater Horizon accident investigation report.” (2010), https://www.bp.com/content/dam/bp/pdf/sustainability/issuereports/ Deepwater_Horizon_Accident_Investigation_Report.pdf – access on 6/11/2018.
3. De Felice F. et al.: Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures. Decision Making, Theory, and Practice, Springer, Cham 2018. DOI: 10.1007/978-3-319-62319-1.
4. Di Bucchianico G. et al.: Human Factors in Transportation: Social and Technological Evolution Across Maritime, Road, Rail, and Aviation Domains. Series: Industrial and Systems Engineering Series. ISBN 9781498726177. CRC Press. 2016.
5. Guastello S.: Human Factors Engineering and Ergonomics: A Systems Approach. CRC Press. 2013.
6. https://www.ntnu.edu/documents/1272224149/0/Keynote+lecture+Patrick+Hudson.pdf/12606dfb-ee30-4175-98bc-807ff5857501 - access on 6.11.2018.

7. https://www.ntnu.edu/documents/1272224149/0/Keynote+lecture+Roar+Thon+-+Cybersecurity.pdf/7f7716f2-b737-4451-bb72-609476684054 - access on 6.11.2018.
8. https://www.ntnu.edu/documents/1272224149/0/keynote-lecture-ali-mosleh.pdf/c324fe37-ab05-4f8c-8a77-fd23a1c7d3af - access on 6.11.2018.
9. https://www.ntnu.edu/documents/1272224149/0/keynote-lecture-sam-mannan.pdf/e87c67bd-d09f-4aa7-83d4-a5fc6ce49195 - access on 6.11.2018.
10. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf – access on 27/08/2019.
11. Haugen S., et al.: Safety and Reliability – Safe Societies in a Changing World. Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway. CRC Press, London, 2018. eBook. DOI 10.1201/9781351174664
12. Hudson P. (2014). Accident causation models, management and the law. Journal of Risk Research. 17. 10.1080/13669877.2014.889202.
13. Hyatt N.: Guidelines for Process Hazadrs Analysis (PHA, HAZOP), Hazard Identification, and Risk Analysis. CRC Press 2003 (first publ.), 2018 (ebook), DOI 10.1201/9781315220376.
14. Kim G. J.: Human–Computer Interaction: Fundamentals and Practice. Auerbach Publications. ISBN 9781482233896. 2015.
15. Kirwan B.: A Guide to Practical Human Reliability Assessment. CRC Press 1994 (first publ.), 2017 (ebook), DOI 10.1201/9781315136349.
16. Kozuba J.: Impact of human factor on likelihood of aircraft accident, [w:] Archives of Transport System Telematics, vol.4, issue 2, May 2011.
17. O'Connor P. (2002), Practical Reliability Engineering (Fourth Ed.), John Wiley & Sons, New York.
18. Rausand, M. et al.: System Reliability Theory: Models, Statistical Methods, and Applications. Wiley Series in Probability and Statistics - Applied Probability and Statistics Section. Wiley. 2003.
19. Salmon P., Regan M., Johnston I.: Human error and road transport., phase one – literature review. Report 256, Monasch University Accident Research Centre, Clayton, Victoria, Australia, Dec. 2005.
20. Smith P., et al.: Human error analysis of the Macondo well blowout. Process Safety Progress 32.2 (2013): 217-221.
21. Shorrock S., Williams C.: Human Factors and Ergonomics in Practice: Improving System Performance and Human Well-Being in the Real World. Auerbach Publications. 2016.
22. Marek T. at. al.: Human Factors of a Global Society: A System of Systems Perspective. Series: Ergonomics Design & Mgmt. Theory & Applications. CRC Press. 2018.
23. The Human Factors Case: Guidance for Human Factors Integration, 29.06.2007 (07/06/22-35) EUROCONTROL, ed. II.
24. US Chemical Safety and Hazard Investigation Board (CSB) "Investigation report overview: Explosion and fire at the Macondo well." (2014). Retrieved from https://www.csb.gov/macondo-blowout-and-explosion/ – access on 6/11/2018.

25. Winter D. C., et al.: Interim Report on Causes of the Deepwater Horizon Oil Rig Blowout and Ways to Prevent Such Events. National Academy of Engineering and National Research Council of the National Academies, 2010.
26. Wiegmann D. et al.: A Human Error Approach to Aviation Accident Analysis – The Human Factors Analysis and Classification System, Burlington 2013.

CZYNNIK LUDZKI JAKO ISTOTNY ELEMENT NIEZAWODNOŚCI I BEZPIECZEŃSTWA SYSTEMÓW TECHNICZNYCH

1. Wprowadzenie

W odniesieniu do człowieka używa się wielu definicji niezawodności. Żadna z tych definicji nie bierze pod uwagę specyficznych cech człowieka odróżniających go od obiektu technicznego, takich jak chociażby podmiotowość, wynikająca z jego świadomości. Człowiek realizuje stawiane mu wymagania w sposób świadomy. Potrafi określić stopień swojej zawodności, a także dostrzec konsekwencje niespełnienia tych wymagań. Te cechy, decydujące o unikalnym charakterze ludzkiej niezawodności, stawiają go w uprzywilejowanej pozycji w stosunku do istniejących systemów technicznych. Niestety, są one również zagrożeniem wynikającym z faktu, że zbyt wysokie wymagania mogą przekroczyć możliwości ludzkiej percepcji.

Rozwój technologii i wzrost jakości materiałów konstrukcyjnych sprawiają, że współcześnie funkcjonujące systemy są coraz bardziej niezawodne, podczas gdy zachowanie człowieka wciąż bardzo mocno wpływa na awaryjność tych systemów. Wynika to w dużej mierze z największej słabości natury ludzkiej, objawiającej się tym, że nawet profesjonaliści popełniają błędy [16]. „Błądzić – znaczy być człowiekiem" [26]. Nawet najbardziej zautomatyzowane systemy są podatne na błędy ludzkie. W rezultacie błąd ludzki pozostaje znaczącym czynnikiem ryzyka, który w przemyśle może mieć katastrofalne konsekwencje. Wzrost świadomości konieczności poznania wpływu błędu ludzkiego umożliwia inżynierom eliminację tych błędów w budowanych systemach, a w efekcie ogranicza ryzyko wystąpienia awarii [3–5, 13, 15]. Aby optymalizować niezawodność całego systemu, w odpowiednich analizach niezbędne jest uwzględnienie zarówno aspektów niezawodnościowych sprzętu, jak i wpływu czynnika ludzkiego. Pierwszy z wymienionych elementów, tj. niezawodność sprzętu czy oprogramowania, jest bardzo dobrze poznany i przeanalizowany w procesach projektowania i wytwarzania, podczas gdy niezawodność człowieka jest często pomijana, być może z powodu braku informacji (braku danych) w tym obszarze. Niezawodność człowieka może być

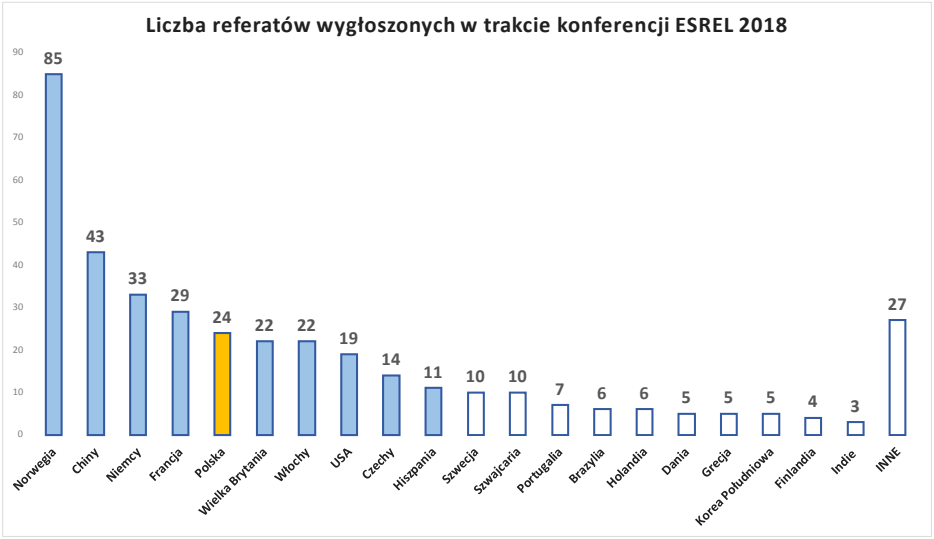
definiowana jako zdolność do wykonywania zadań z minimalnym ryzykiem błędu, w określonych warunkach i określonym czasie [19, 21, 23]. Definicja ta uwzględnia istotne aspekty działania człowieka, takie jak dokładność i szybkość, oraz fakt uzależnienia jakości tego działania od środowiska materialnego. Niezawodność człowieka nie jest opcjonalna dla zrozumienia ogólnej niezawodności systemu, jest wręcz niezbędna [19]. Prowadzenie analizy niezawodności systemów technicznych bez uwzględnienia człowieka jako kluczowego elementu systemu jest podejściem mocno niedoskonałym. Niezbędne jest, żeby wpływ czynnika ludzkiego był integralną częścią prowadzonej analizy niezawodności systemów technicznych. Podczas gdy efektywne działanie człowieka może prowadzić do osiągnięcia zakładanych celów, nieefektywne działanie wywołuje zagrożenie bezpieczeństwa, zwiększa prawdopodobieństwo awarii i wypadków lub w skrajnych przypadkach powoduje śmierć człowieka. Odpowiednio prowadzona analiza niezawodności powinna traktować człowieka jako kluczowy element systemu technicznego i tylko tak prowadzona ma istotne znaczenie dla poprawy bezpieczeństwa całego środowiska [19, 22].

Do osiągnięcia wyznaczonego celu konieczne jest wzięcie pod uwagę trzech istotnych aspektów: świadomości występowania ryzyka, konieczności podejmowania określonych decyzji i poprawności prowadzenia wybranych działań. Powinny być to działania skuteczne, których uzyskane wyniki są zgodne z planowanym celem [17, 18]. Decyzje dotyczące większości działań obarczone są ryzykiem niepowodzenia. W takich sytuacjach istnieje konieczność poszukiwania rozwiązań aż do momentu uzyskania wyników zgodnych z zakładanym celem działania. Podejście to determinuje stosowanie rozwiązań, które muszą uwzględniać wieloaspektową analizę funkcjonowania współczesnych systemów technicznych. Podstawowym celem tych rozwiązań jest zapewnienie bezpieczeństwa działania zarówno procesów wytwarzania, jak i eksploatacji obiektów technicznych [17].

Na rozwiazywanie przedstawionych powyżej problemów była ukierunkowana europejska konferencja dotycząca bezpieczeństwa i niezawodności systemów technicznych ESREL, odbywająca się pod auspicjami Europejskiego Towarzystwa Bezpieczeństwa i Niezawodności (ESRA). Konferencja miała miejsce w dniach 17–21 czerwca 2018 r., w Norweskim Uniwersytecie Nauki i Technologii w Trondheim. ESREL nie jest jedyną na świecie cykliczną konferencją w obszarze niezawodności i bezpieczeństwa, jest natomiast, oprócz PSAM-u (Probabilistic Safety Assessment and Management Conference), konferencją największą pod względem liczby uczestników i prezentowanych referatów. Jej unikatowość to przede wszystkim wieloletnie doświadczenie (28 edycji) oraz bardzo szeroki zakres tematyczny, obejmujący większość aspektów związanych z szacowaniem ryzyka czy niezawodnością i bezpieczeństwem systemów technicznych.

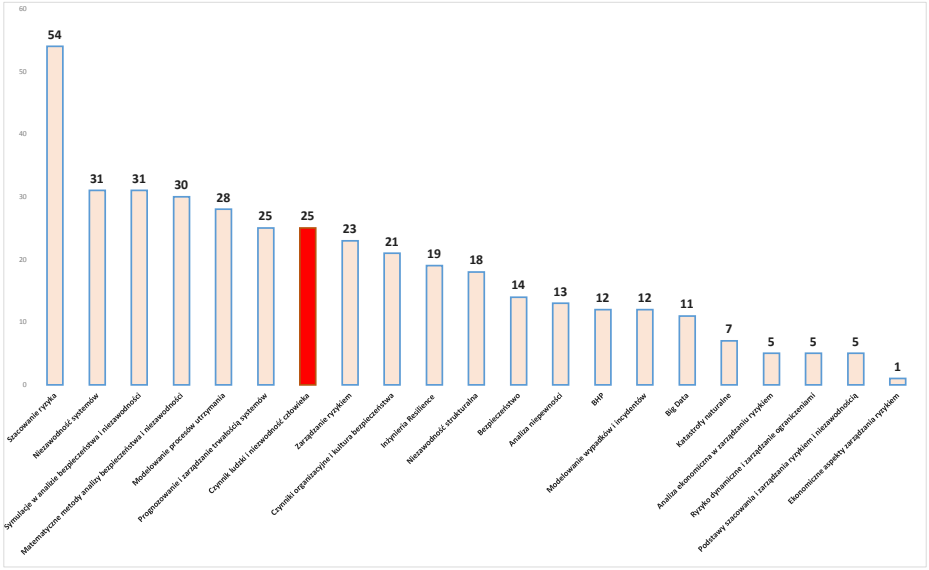
2. Tematyka konferencji ESREL 2018

Tematem przewodnim 28. ESREL-a było „Bezpieczne społeczeństwo w zmieniającym się świecie". Przedstawiono 390 artykułów (rys. 1), wydanych w materiałach konferencyjnych, dostępnych po raz pierwszy w historii w systemie *open access*. W konferencji uczestniczyli przedstawiciele 47 różnych krajów – grupa „INNE" obejmuje 27 krajów, z których zgłoszono po jednym referacie konferencyjnym. Najwięcej referatów wygłosili przedstawiciele Norwegii oraz Chin. Polska pod względem liczebności artykułów uplasowała się na piątym miejscu.



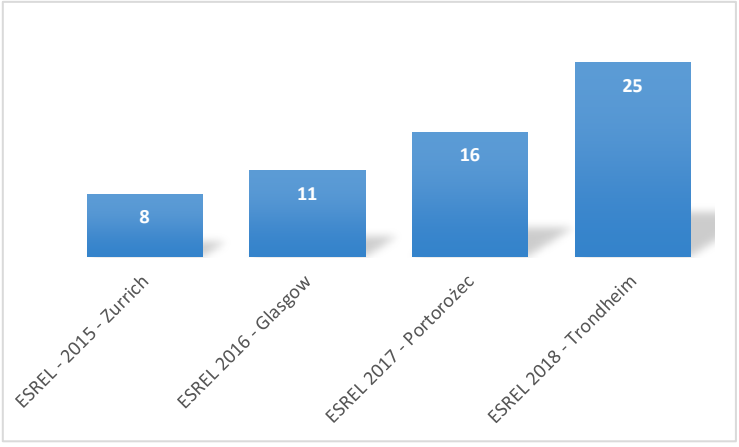
Rys. 1. Liczba referatów wygłoszonych przez przedstawicieli poszczególnych państw – na podstawie [11]

Konferencja obejmowała 21 zakresów metodologicznych obszarów zastosowań (rys. 2). Stanowiła forum prezentacji i dyskusji na tematy prac naukowych dotyczących teorii, technik, metod i osiągnięć związanych ze wskazanymi problemami.



Rys. 2. Liczba referatów w poszczególnych obszarach metodologicznych i obszarach zainteresowań ESREL 2018 – na podstawie [11]

Oprócz wiodących od lat obszarów konferencji ESREL, tj. szacowania ryzyka, analizy ryzyka czy też metod matematycznych i badań symulacyjnych w opisie ryzyka i bezpieczeństwa systemów technicznych, warto zwrócić uwagę na rosnące zainteresowanie obszarem dotyczącym wpływu czynnika ludzkiego na funkcjonowanie tych systemów (rys. 3).



Rys. 3. Liczba referatów w obszarach dotyczących wpływu czynnika ludzkiego (HF) na ostatnich konferencjach ESREL

Ze statystycznego punktu widzenia tegoroczny ESREL prezentował się następująco:

- odbyło się łącznie 101 sesji – w tym 5 tematycznych sesji specjalnych:
  1. Bezpieczeństwo i analiza ryzyka w systemach autonomicznych I.
  2. Bezpieczeństwo i analiza ryzyka w systemach autonomicznych II.
  3. Bezpieczeństwo w obszarach arktycznych.
  4. Bezpieczeństwo i analiza ryzyka w systemach autonomicznych III.
  5. Bezpieczeństwo i analiza ryzyka w systemach technicznych.
- dodatkowo 2 sesje specjalne w obszarze zastosowań (aplikacji) dla przemysłu:
  1. Zarządzanie ryzykiem kolizji w operacjach morskich.
  2. Wyzwania dla przemysłu w celu poprawy bezpieczeństwa i niezawodności systemów kolejowych.
  3. Warsztaty: Wieloaspektowe systemy bezpieczeństwa – przykłady zastosowań.

3. Wpływ czynnika ludzkiego na poprawność funkcjonowania wybranych systemów technicznych

Analiza wpływu czynnika ludzkiego na poprawność funkcjonowania systemów technicznych polega na określaniu, w jakim stopniu ludzka wydajność, stan psychofizyczny, wiedza i umiejętności ogólne i specjalistyczne oraz relacje interpersonalne w grupie mogą negatywnie wpływać na system; przewidywaniu, jak często będzie to miało miejsce oraz identyfikacji potencjalnych konsekwencji, jeśli takie wystąpią [19]. Wiedza ta jest wykorzystywana do optymalizacji bezpieczeństwa systemu. Analizy służą do podejmowania decyzji zarówno w istniejących, jak i nowo projektowanych systemach, gdy ryzyko jest wysokie i musi być uwzględnione na poziomie decyzyjnym. W przypadku istniejących systemów badanie wpływu czynnika ludzkiego służy do oceny problemów, które należy poprawić, i do tworzenia możliwych aktualizacji systemów. W przypadku systemów, które nie zostały zbudowane, służy do oceny projektów koncepcyjnych [22].

Analiza niezawodności człowieka pokazuje, że każdy system techniczny ma inne wymagania i inaczej wpływa na ludzką niezawodność. Dlatego niezbędne jest wykorzystywanie wszystkich dostępnych narzędzi i metod (wykorzystanie inżynierii systemów i metod nauk behawioralnych) w kontekście oceny interakcji między ludźmi a pozostałymi komponentami systemu oraz umożliwienia zarządzania błędami ludzkimi w celu optymalizacji niezawodności systemu i zmniejszenia

ryzyka [5]. Doskonałym odzwierciedleniem powyższych stwierdzeń była problematyka poruszana przez *keynote speakerów* w wykładach plenarnych ESREL-a. Wykłady dotyczyły następujących obszarów [6–9]:

- roli człowieka w zapewnieniu odpowiedniego poziomu bezpieczeństwa cybernetycznego;
- roli wiedzy eksperckiej (czynnika ludzkiego) w szacowaniu ryzyka;
- nowatorskich sposobów zarządzania ryzykiem;
- innowacyjnych technologii w pozyskiwaniu i opracowywaniu bogactw naturalnych z morskich złóż głębinowych.

Wspólnym mianownikiem wszystkich wymienionych wykładów był wpływ człowieka na funkcjonowanie współczesnego świata i otaczającego go środowiska.

Współczesny świat to wszechobecna technologia, a z nią jest ściśle powiązany problem bezpieczeństwa w cyberprzestrzeni. Należy zatem przeprowadzić analizę roli człowieka w zapewnieniu odpowiedniego poziomu bezpieczeństwa cybernetycznego w dużych organizacjach [1]. W pierwszej kolejności należy odpowiedzieć na pytanie, dlaczego cyberbezpieczeństwo stanowi tak istotny problem i to właśnie na jego aspektach powinna się koncentrować uwaga zarządzających systemami. Według Global Risk Report z 2018 r. [10], cyberbezpieczeństwo uplasowało się na trzecim miejscu wśród największych zagrożeń bezpieczeństwa człowieka, po degradacji środowiska naturalnego i zagrożeniach ekonomicznych [7]. Nie podlega dyskusji fakt, że bez technologii współczesne środowisko nie jest w stanie poprawnie funkcjonować. Z jednej strony ułatwia życie, a z drugiej stanowi główne źródło zagrożeń. Kluczową rolę w funkcjonowaniu każdego systemu technicznego odgrywa człowiek [14]. I to on w wielu przypadkach jest najsłabszym ogniwem systemu. „Zaczynamy myśleć o technologii. Łączymy tę technologię z bezpieczeństwem. Myślimy o zaporach ogniowych, programach antywirusowych, hasłach itp. Wszystko to układa się w napis cyberbezpieczeństwo! Ale mamy tendencję do zapominania o jednym najważniejszym, kluczowym czynniku – człowieku!" [7] – w taki sposób zdefiniowano problem funkcjonowania człowieka w zarządzaniu systemami technicznymi. Według prowadzonych w USA badań, 84% wszystkich cyberataków jest spowodowane błędami lub zaniedbaniami ze strony człowieka [14]. Te dane świadczą o tym, że cyberbezpieczeństwo jest problemem na tyle poważnym, że stanowi podmiot zainteresowania rządów największych państwa świata. Najpoważniejszym wyzwaniem zarządzających systemami wydaje się znalezienie równowagi między bezpieczeństwem a prywatnością, po to aby nadal cieszyć się technologią i wykorzystywać jej możliwości. Niezbędne jest zrozumienie zarówno procesów występujących w każdym systemie technicznym (w tym technologii), ale jeszcze istotniejszym elementem jest

zrozumienie potrzeb człowieka i zagrożeń w sieci powiązań: człowiek – maszyna – system techniczny [1, 14].

Innym spojrzeniem na rolę czynnika ludzkiego jest problematyka wykorzystania wiedzy eksperckiej w szacowaniu ryzyka. „Niemożliwe wręcz wydaje się znalezienie analizy ryzyka i niezawodności, która nie opierałaby się na opinii ekspertów. To z kolei stanowi fakt, który jest często wymieniany jako słabość i źródło wątpliwości co do wiarygodności tak prowadzonych analiz" [8]. Wśród głównych problemów dotyczących wątpliwości analiz eksperckich wskazano pięć głównych czynników:

- kwalifikacje eksperta prowadzącego analizę,
- dobór procedury szacowania,
- poprawność procesu pozyskiwania wiedzy,
- wybór metody agregacji,
- dostępne informacje dotyczące kalibracji (np. historyczna wiedza na temat wydajności ekspertów).

Sformułowano również zbiór zasad postępowania, który minimalizuje wpływ subiektywizmu na formułowanie opinii eksperckich [8]:

1. Zbiór opinii wielu ekspertów daje bardziej dokładne wyniki niż opinia pojedynczego eksperta (zasada *n-heads*).
2. Matematyczne metody agregacji są na ogół lepsze od metod behawioralnych.
3. Jakość opinii można znacznie poprawić, rozkładając złożony problem na szereg bardziej elementarnych problemów.
4. Zauważalna jest znaczna poprawa osiąganych wyników, jeżeli już na etapie wstępnej definicji problemu i jego rozkładu wykorzystujemy konsultacje z ekspertami.

Kolejnym aspektem poddawanym analizie w zakresie ważności wpływu czynnika ludzkiego na jego funkcjonowanie jest zarządzanie ryzykiem zarówno w obszarach standardowo badanych, jak i w obszarach, które powszechnie są pomijane w trakcie prowadzonych analiz (rys. 4).

Rys. 4. Podział czynników wpływających na powstawanie wypadków [6]

Najbardziej popularne metody zarządzania ryzykiem wykorzystują dość ograniczony zestaw powodów lub przyczyn je wywołujących. Większość potencjalnych incydentów, ok. 80%, może wynikać z przyczyn liniowych i deterministycznych. Z pozostałych 20% – 80% przyczyn może być coraz bardziej nieliniowych, ale nadal deterministycznych. Sumarycznie daje to 96% [6]. Pozostałe potencjalne wypadki będą miały przyczyny, które są zarówno nieliniowe, jak i niedeterministyczne, czyli mały zestaw, który nazywany jest WEIRD – Wildly Erratic Incidents Resulting in Disaster [12].

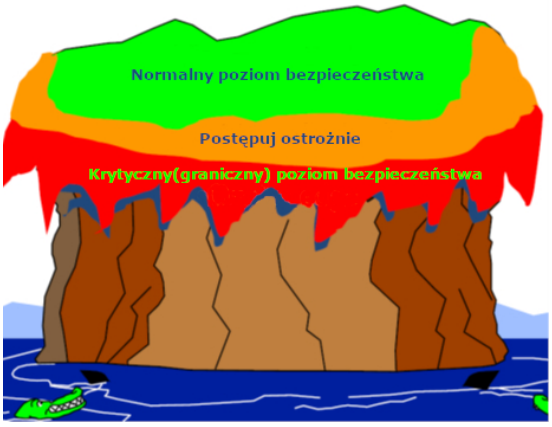
Wszystkie przyczyny wypadków można zaliczyć do jednej z trzech podstawowych grup:

- typ I – definiowane prostymi modelami obejmującymi swym zasięgiem 80% wszystkich wypadków – zwykłe wypadki osobiste;
- typ II – kolejny krok to 80% reszty, czyli łącznie 96% – złożone wypadki osobiste i niektóre wypadki organizacyjne;
- typ III – kolejny krok to 80% reszty, czyli łącznie 99,2% – złożone wypadki procesowe i organizacyjne.

Do każdej z trzech podstawowych grup została przypisane obszary odpowiedzialności, jaka spoczywa na poszczególnych szczeblach zarządzających organizacją [5]:

- typ I – bezpośredni, nakłada odpowiedzialność na indywidualną kontrolę pojedynczego pracownika;
- typ II – kierownictwo kontroluje warunki, w których pracujemy; kierownictwo większą uwagę skupia na organizacji i ma mniejszą kontrolę nad jednostkami;
- typ III – obejmuje tylko ten obszar, który jest w zakresie kontroli kierownictwa najwyższego szczebla; kierownictwo tego szczebla ustala cele i standardy pracy jaką wykonujemy.

Szczególną uwagę w zakresie problematyki powstawania wypadków skoncentrować należy na branży lotniczej. W lotnictwie komercyjnym i niektórych innych branżach poważne wypadki są obecnie zjawiskiem niezwykle rzadkim. Proste modele oceny ryzyka i analizy często nie potrafią uchwycić, w jaki sposób wypadki te są spowodowane. Rozwiązaniem omówionego problemu może być zbiór przyczynowo-skutkowy zdefiniowany jako WEIRD. Kluczem do rozwiązywania wypadków rzadkich jest zrozumienie przestrzeni ryzyka, a rozwiązaniem stosowanie tzw. reguły trzech [6]. Wypadki są złożonymi zdarzeniami, składającymi się z ponad 50 bezpośrednich i dodatkowych czynników. Eliminacja pojedynczego czynnika może zapobiec wypadkowi, ale może być 49+ innych czynników czekających, tzw. „an Accident Waiting to Happen” [6]. Reguła trzech pomaga rozwinąć świadomość sytuacyjną zarówno na poziomie organizacji, jak i w przypadku indywidualnym. Świadomość sytuacyjna mówi nam, jak blisko „krawędzi” znajduje się nasza organizacja (rys. 5).



Rys. 5. Poziomy bezpieczeństwa w regule trzech [6]

Reguła trzech jest oparta na dwóch poziomach granicznych – zielonym i pomarańczowym [6]:

- zielony – prowadź dalej swoje działania;
- pomarańczowy – postępuj ostrożnie;
- czerwony – bezwzględnie przerwij działania i zajmij się kompleksową analizą problemu,

przy czym należy pamiętać o zasadzie: trzy pomarańczowe to jeden czerwony, czyli wymagane jest bezwzględne przerwanie działań.

Analizując wpływ działalności człowieka na otaczające systemy oraz prowadząc analizę wpływu błędów ludzkich na zmiany czy degradacje tych systemów, nie sposób pominąć problematykę środowiska naturalnego, w tym środowiska morskiego. Jednym z największych zagrożeń dla środowiska morskiego jest dynamiczny rozwój innowacyjnych technologii pozyskiwania i opracowywania złóż głębinowych. Wykorzystywane współcześnie technologie obarczone są wysokim ryzykiem i mają wyjątkowo niebezpieczny charakter [9]. Charakter ten jest źródłem nowych, unikalnych i nieznanych człowiekowi dotychczas zagrożeń. Po incydencie Transocean Deepwater Horizon i wycieku ropy naftowej w Zatoce Meksykańskiej, Biuro Bezpieczeństwa Wewnętrznego Departamentu Spraw Wewnętrznych Stanów Zjednoczonych sfinansowało Ocean Energy Safety Institute na Texas A&M University [2, 24, 25]. Jednocześnie wiele innych organizacji zwiększyło wysiłki w zakresie rozwiązywania problemów związanych z systemami zarządzania i technologiami zapewniającymi bezpieczniejsze i bardziej przyjazne dla środowiska operacje w zakresie pozyskiwania energii oceanicznej [2]. Wśród głównych kierunków działania w zakresie poprawy bezpieczeństwa prowadzenia operacji pozyskiwania złóż głębinowych wskazano [9]:

- rozwój metod wykrywania wczesnych ruchów tektonicznych,
- wprowadzenie zaawansowanych materiałów do warunków HPHT (*high pressure high temeperature*),
- zapobieganie korozji,
- wykrywanie wycieków podmorskich,
- rozwój sprzętu do kontroli ciśnienia o wysokiej wydajności,
- rozwój metod prowadzenia izolacji strefowej,
- ograniczanie wycieków i łagodzenie ich skutków,
- integracja aspektów technicznych, organizacyjnych i społecznych prowadzonych działań – eliminacja błędów ludzkich (*human factor*).

4. Podsumowanie

Człowiek ma decydujący wpływ na bezpieczną eksploatację systemów technicznych, a jego działalność jest kluczowa z punktu widzenia poprawności funkcjonowania wszystkich otaczających systemów, w tym tak wrażliwych i skomplikowanych jak środowisko naturalne. Analiza niezawodności systemu technicznego nie może pomijać niezawodności człowieka. Dlatego też problematyka niezawodności człowieka musi być integralną częścią analizy niezawodności systemów. Potencjalne błędy człowieka zwiększają poziom ryzyka związanego z eksploatacją każdego systemu. Mimo ogólnie przyjętych metod służących do prowadzania analiz niezawodności człowieka, istnieją duże trudności w precyzyjnej ocenie wpływu czynnika ludzkiego na poziom bezpieczeństwa. Wielu ekspertów uważa, że aktualne stosowane metody są zbyt mało szczegółowe i zbyt mocno uproszczają koncepcję błędów człowieka, dlatego też cały czas trwają prace nad nowymi rozwiązaniami. W artykule wskazano na potrzebę uwzględnienia w tych metodach podmiotowego charakteru człowieka, co wynika z jego świadomości. Człowiek realizuje zadania w sposób świadomy, ma zdolność oceny zmieniającej się sytuacji, zdolność do działania w nietypowych sytuacjach, uczenia się na swoich i cudzych błędach oraz kreatywność w rozwiązywaniu problemów. Natura ludzka ma jednak swoje ograniczenia. Dlatego też w analizie niezawodności człowieka niezbędne jest większe zwrócenie uwagi na prawa rządzące psychiką i zachowaniem ludzkim, czyli uwzględnianie również aspektu psychologicznego. Jednym z najtrudniejszych elementów do rozwiązania jest sformułowanie kryteriów mierzalności ludzkich zachowań. Opisanie językiem matematyki zachowania człowieka w sytuacjach kryzysowych to bez wątpienia najważniejsze wyzwanie dla naukowców na najbliższą przyszłość.

5. Literatura

1. Boy E.: The Handbook of Human-Machine Interaction: A Human-Centered Design Approach. ISBN 9781138075825. CRC Press. 2017.
2. BP, “Deepwater Horizon accident investigation report.” (2010), https://www.bp.com/content/dam/bp/pdf/sustainability/issuereports/Deepwater_Horizon_Accident_Investigation_Report.pdf – dostęp 6/11/2018.
3. De Felice F. et al.: Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures. Decision Making, Theory, and Practice, Springer, Cham 2018. DOI: 10.1007/978-3-319-62319-1.

4. Di Bucchianico G. et al.: Human Factors in Transportation: Social and Technological Evolution Across Maritime, Road, Rail, and Aviation Domains. Series: Industrial and Systems Engineering Series. ISBN 9781498726177. CRC Press. 2016.
5. Guastello S.: Human Factors Engineering and Ergonomics: A Systems Approach. CRC Press. 2013.
6. https://www.ntnu.edu/documents/1272224149/0/Keynote+lecture+Patrick+Hudson.pdf/12606dfb-ee30-4175-98bc-807ff5857501 - dostęp 6.11.2018.
7. https://www.ntnu.edu/documents/1272224149/0/Keynote+lecture+Roar+Thon+-+Cybersecurity.pdf/7f7716f2-b737-4451-bb72-609476684054 - dostęp 6.11.2018.
8. https://www.ntnu.edu/documents/1272224149/0/keynote-lecture-ali-mosleh.pdf/c324fe37-ab05-4f8c-8a77-fd23a1c7d3af - dostęp 6.11.2018.
9. https://www.ntnu.edu/documents/1272224149/0/keynote-lecture-sam-mannan.pdf/e87c67bd-d09f-4aa7-83d4-a5fc6ce49195 - dostęp 6.11.2018.
10. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf – dostęp 27/08/2019.
11. Haugen S., et al.: Safety and Reliability – Safe Societies in a Changing World. Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway. CRC Press, London, 2018. eBook. DOI 10.1201/9781351174664
12. Hudson P. (2014). Accident causation models, management and the law. Journal of Risk Research. 17. 10.1080/13669877.2014.889202.
13. Hyatt N.: Guidelines for Process Hazadrs Analysis (PHA, HAZOP), Hazard Identification, and Risk Analysis. CRC Press 2003 (first publ.), 2018 (ebook), DOI 10.1201/9781315220376.
14. Kim G. J.: Human–Computer Interaction: Fundamentals and Practice. Auerbach Publications. ISBN 9781482233896. 2015.
15. Kirwan B.: A Guide to Practical Human Reliability Assessment. CRC Press 1994 (first publ.), 2017 (ebook), DOI 10.1201/9781315136349.
16. Kozuba J.: Impact of human factor on likelihood of aircraft accident, [w:] Archives of Transport System Telematics, vol.4, issue 2, May 2011.
17. O'Connor P. (2002), Practical Reliability Engineering (Fourth Ed.), John Wiley & Sons, New York.
18. Rausand, M. et al.: System Reliability Theory: Models, Statistical Methods, and Applications. Wiley Series in Probability and Statistics - Applied Probability and Statistics Section. Wiley. 2003.
19. Salmon P., Regan M., Johnston I.: Human error and road transport., phase one – literature review. Report 256, Monasch University Accident Research Centre, Clayton, Victoria, Australia, Dec. 2005.
20. Smith P., et al.: Human error analysis of the Macondo well blowout. Process Safety Progress 32.2 (2013): 217-221.
21. Shorrock S., Williams C.: Human Factors and Ergonomics in Practice: Improving System Performance and Human Well-Being in the Real World. Auerbach Publications. 2016.

22. Marek T. at. al.: Human Factors of a Global Society: A System of Systems Perspective. Series: Ergonomics Design & Mgmt. Theory & Applications. CRC Press. 2018.
23. The Human Factors Case: Guidance for Human Factors Integration, 29.06.2007 (07/06/22-35) EUROCONTROL, ed. II.
24. US Chemical Safety and Hazard Investigation Board (CSB) "Investigation report overview: Explosion and fire at the Macondo well." (2014). Retrieved from https://www.csb.gov/macondo-blowout-and-explosion/ – access on 6/11/2018.
25. Winter D. C., et al.: Interim Report on Causes of the Deepwater Horizon Oil Rig Blowout and Ways to Prevent Such Events. National Academy of Engineering and National Research Council of the National Academies, 2010.
26. Wiegmann D. et al.: A Human Error Approach to Aviation Accident Analysis – The Human Factors Analysis and Classification System, Burlington 2013.