STATE OF KNOWLEDGE ON RELIABILITY AND SAFETY IN THE LIGHT OF THE SCIENTIFIC CONFERENCES IN 2017

STAN WIEDZY O NIEZAWODNOŚCI I BEZPIECZEŃSTWIE W ŚWIETLE KONFERENCJI NAUKOWYCH W 2017 R.

Marek Młyńczak, Tomasz Nowakowski

Wrocław University of Science and Technology, Faculty of Mechanical Engineering
Politechnika Wrocławska, Wydział Mechaniczny

Abstract: The presented analysis of state of knowledge on reliability and safety is based on publications of 27th European Safety and Reliability Conference ESREL 2017, which took place in Portoroz in Slovenia on 18-22 June 2017 and 52nd and 49rd Seminars of ESReDA European Safety, Reliability and Data Association which were held, respectively: at Vytautas Magnus University in Kaunas, Lithuania (29-31 May 2017) and at European Commission Joint Research Center, Ispra, Italy (13-15 November 2017).

Keywords: reliability, safety, conferences, 2017

Streszczenie: Przedstawiona analiza stanu wiedzy o niezawodności i bezpieczeństwie bazuje na publikacjach zaprezentowanych na corocznej 27 Europejskiej Konferencji Bezpieczeństwa i Niezawodności ESREL 2017, która odbyła się w dniach 18 – 22 czerwca 2017 roku w Portoroz na Słowenii oraz na referatach wygłoszonych w trakcie 52 i 53 seminarium ESReDA (European Safety, Reliability and Data Association), które odbyły się, odpowiednio: 29 – 31 maja 2017 r. w Kownie (Litwa) Uniwersytecie Witolda Wielkiego oraz 13 – 15 listopada 2017 r. w Ispra (Włochy) w European Commission Joint Research Center.

Słowa kluczowe: bezpieczeństwo, niezawodność, konferencja, 2017 r.
STATE OF KNOWLEDGE ON RELIABILITY AND SAFETY IN THE LIGHT OF THE SCIENTIFIC CONFERENCES IN 2017

1. Conference ESREL 2017

Introduction

The 27th ESREL conference took place in 2017 in Portorož, on a patch of the tiny Slovenian coast. The distance between extreme points on the coast is about 20 km, and as expanded, it is of almost 50 km. The resort town is located next to the well-known tourist and historically town of Piran. The conference proceedings were placed in 5* located between Portorož and Piran. The Grand Hotel Bernardin held all conference events from registration, through lectures and sessions, to diner and the exhibition of security works under the slogan "Images of Risk. The submitted works could be photographs, posters, and artistic compositions emphasizing the aspects of threats to man and the natural environment.

During the four-day conference, five plenary lectures were delivered, 96 sessions, 3 practical workshops and 7 special sessions. Parallel sessions took place in 5 rooms. The conference did not have a slogan this year, although due to the organizers, there was a large thematic focus on issues related to energy, mainly nuclear. The works were double reviewed by 122 members of the technical committee and published in the publishing house CRC Press, Taylor & Francis Group with the ISBN number [5].

The conference was supported by a smartphone application that allows for the management of the conference program and its time, both for the organizers and participants.

The conference structure distinguishes two categories of scientific areas. These areas coincide with research teams in the structure of the ESRA organization. In the area of research methodology there are the following active teams:

- Accident and Incident Modeling,
- Economic Analysis in Risk Management,
- Foundational Issues in Risk Assessment and Management,
- Human Factors and Human Reliability,
- Maintenance Modeling and Applications,
- Mathematical Methods in Reliability and Safety,
- Prognostics and System Health Management,
- Resilience Engineering,
- Risk Assessment,
- Risk Management,
- Simulation for Safety and Reliability,
- Structural Reliability,
- System Reliability,
- Uncertainty Analysis.
Thematic areas concerning industrial technologies and practical applications are focused on:
- Aeronautics and Aerospace,
- Chemical and Process Industry,
- Civil Engineering,
- Critical Infrastructures,
- Energy,
- Information Technology and Telecommunications,
- Land Transportation,
- Manufacturing,
- Maritime and Offshore Technology,
- Natural Hazards,
- Nuclear Industry,
- Occupational Safety,
- Security.

The organizers provided a series of five ordered lectures delivered in plenary sessions. The lecturers were specialists in their fields of scientific work:
- Dr. Andrej Stritar, director of the Slovenian Nuclear Safety Administration, title of the lecture: Risk, Threat, Security, Reliability - how to use these concepts to ensure that nothing went wrong in the nuclear installation.
- Dr. Stefan Hirschberg, Energy Systems Analyses Laboratory, Paul Scherrer Institute (PSI), Villigen PSI, Switzerland, lecture title: Health hazards in energy installations. The speech concerned various aspects of the impact of various energy systems on human health. He presented the methodology of assessment based on Life Cycle Assessment (LCA) and Impact Pathway Approach (IPA) in relation to nuclear, gas, coal, solar, wind or water wave plants.
- Professor Enrique Lopez Droguett, Universidad De Chile, Chile, lecture title: On the challenges and treatment of uncertainty in modelling. Based on a historical sketch, the speaker developed a philosophical approach to uncertainty. He discussed the uncertainty of forecasting by pointing to modelling as a source of uncertainty (uncertainty related to the adequacy of the model to reality) and parametric uncertainty (uncertainty of the possibility of parametric description of reality).
- Prof. Daniel Straub, Technische Universität München, Germany, lecture title: Reliability of intelligent technical systems. The lecture touched upon problems related to the threats of intelligent technical systems, where human participation in operating such objects is to be small. Autonomous vehicles and machines require precise and reliable diagnostic systems for reacting in the event of unwanted conditions. The author presented an effective risk assessment method based on the Bayesian analysis. He presented the use of the method in relation to large data sets for risk management in autonomous facilities.
- Professor Antoine Rauzy, Norwegian University of Science and Technology, Norway, lecture title: AltaRica 3.0: Implementation of a model risk assessment. The lecture concerned the use of the third version of the AltaRica 3.0 language object oriented for RAMS analysis. The aim of this activity is to develop a tool for assessing the efficiency of complex systems using stochastic processes.
Other, scientific conference events were workshops, special sessions and a discussion panel:

- Discussion workshop on Applications and use of risk assessment - key challenges and current achievements,
- Workshops sponsored by HBM PRENSCIA (formerly ReliaSoft): Integration of reliability and durability in HBM PRENSCIA software,
- Workshops sponsored by BQR: Effective engineering of reliability in advanced design and unmanned facilities,
- Special session: Critical Infrastructure Safety organized by prof. Krzysztof Kołowroc
- Special session: Truss structures, Marie Skłodowska-Curie Innovative Training Network on structural reliability, PRENSCIA.
- Special session: ASAMPSA_E Advanced risk assessment methodology, developed PSA.
- Special session: RAMS in the railways: theory and practice.
- Special session: Challenges in land transport.
- Special session: Analysis and risk management using BIG DATA.
- Special session: Reliability and safety engineering based on modelling.

Statistics of conference participants

Interest in the ESREL 2017 conference was reported to the conference system at the end of 2016 by around 700 people, over 640 summaries of articles were declared, of which 480 were submitted, and 455 (441 in 2016) full texts of the papers were finally adopted. Fig. 1 shows the histogram of participants by countries. Over 640 people from 49 countries reported interest.

Fig. 1 Participation of national teams in the ESREL 2017 conference
About 450 people from 34 countries were real participants (Fig. 2), with 75% of participants coming from European countries.

**Fig. 2 Distribution of ESREL 2017 conference participants according to nationalities.**

**Discussion presented in the panel Industrial Challenges in Land Transportation**

The Monday discussion panel dealt with the problems of maintaining the Alstom vehicle fleet and was moderated by Bob Huisman. Pierre Dersin presented the presentation on Maintenance of fleet vehicles as a dynamic decision process (Fleet Maintenance as a Dynamic Decision Process). Pierre Dersin pointed to the need to change the service strategy from object to fleet. A single object requires preventive maintenance to avoid sudden damage, and repairs should be made according to the "as old, as new" strategy (100% exploded potential after repair). It is necessary to monitor the operation, in particular the handling, the working loads and the ambient conditions. In the state model of the damage process, a three-state system was adopted: the state of fitness, the state of partial degradation and the state of inability. One of Alstom's main goals is to determine the reliable amount of remaining operational potential (RUL - remaining useful lifetime), assuming the minimum total costs of preventive and corrective maintenance, including external costs after damage. The planned method of achieving this goal is monitoring the technical condition (collecting physical data from vehicles), determining the current state and forecasting the progress of the degradation process.

The company assumes that by 2037 all vehicles will be monitored on-line in real time, service will be determined dynamically depending on the condition of each facility, estimation of service costs will be carried out automatically in service stations. The service centre will manage the service process for the entire fleet of vehicles in accordance with the cost minimization model while ensuring the desired level of rolling stock readiness. However, the future solution may be decentralized handling, i.e.: data processing carried out locally (vehicle) or send pre-processed data or raw data to the centre if a satisfactory solution cannot be obtained locally.
2. Seminar ESReDA

The 52nd ESReDA seminar [8] was devoted to the issues of readiness and resistance to critical infrastructure (CI) interference. 17 papers divided into 5 sessions, 2 plenary sessions and a round table discussion were presented. The individual sessions concerned: risk and emergency management, tasks related to securing critical infrastructure, security systems engineering, modelling and simulation of readiness, resilience and vulnerability of systems. Round table discussions were devoted to the problems of cybersecurity of critical infrastructure. The readiness and resilience of critical infrastructure is the main challenge for social security in the modern world [8]. Critical infrastructure provides key services to a modern society. Some of CI's distortions may endanger the security of the citizen, the security of strategic resources, and even the continuity of management.

The importance of CI has been recognized by the European Commission by issuing Directive 2008/114/EC on the identification and designation of European CIs and the assessment of the need to improve their protection. The European Program for the Protection of European Critical Infrastructure (EPCIP) has been developed and operated since 2006. The program includes preliminary projects analysing EU gas and electricity systems and other CI. The European Commission Joint Research Centre is actively involved in EPCIP, providing technical support, dissemination and training activities.

The key role that CI's play in the security of modern societies is a direct result of the fact that the importance of information technology (IT) is constantly growing for every smallest task carried out in the everyday life of a human being. Constant progress in the field of IT forces modern systems and infrastructures to be more intelligent, distributed and proactive. It increases the productivity, prosperity and living standards of modern societies. But it also increases the complexity of systems and infrastructure. The more complex the system is, the more vulnerable it is to threats that may affect its functionality. Losing the functionality of critical infrastructure can cause major crises in modern societies. To counteract the increase of systems vulnerability, the activity in the phases of designing, manufacturing and operation of systems should be aimed at improving the system's readiness and resistance to various threats.

The presentation [1] drew attention to the implications of changes in the cyberspace environment that have occurred over the past few years and which currently require a response in the form of mutual understanding, moderation, acceptance of responsibility, transparency and cooperation to deal with new threats. The cyber-security problem began [1] from dealing with the first hackers attacking information systems with viruses, such as the Michelangelo virus from 1991. Currently, apart from socially motivated hackers and cyber-terrorists, we are dealing with sponsored by various states cyber-attacks not limited to IT systems.
The emergence of STUXNET, the "denial of computers" attack on the Saudi Aramco energy company and cyber-crimes that took place in one of the regional energy networks in Ukraine in the winter of 2015, clearly showed that critical infrastructure that supports national economies and the well-being of modern society has become an increasingly attractive target for cyber-attacks. In addition, the extension of the capabilities of modern industrial control systems (ICS), made possible by advances in information and communication technologies (ICT) and their application to the management of complex critical infrastructure systems, in addition to increased efficiency and savings, created a number of significant interdependencies and vulnerabilities. This vulnerability, due to a lack of understanding of the interconnectedness of increasingly complex systems, caused unintentional incidents. Vulnerabilities, if known to criminals, can be used to carry out intended cyber-attacks; activities that are now possible thanks to the introduction of IT in the previously isolated and proprietary world of industrial control systems (SCADA). New threats resulting from cyberspace have provided new and extensive challenges that exceed the national level to the international level. Critical infrastructure today has a cross-border or international dimension. The threat at the national level may affect the infrastructure of the neighbouring country. While some governments and industries take important and effective actions in the field of laws, regulations and norms, they do not notice the international dimension of today's cyber threats. SCADA and ICS environments can no longer be considered safe against today's dynamic cyber threats. Although the importance of transport infrastructure in crisis management is recognized, it is believed that the role of critical infrastructure operators (CIs) must still be fully formalized, especially when it comes to providing assistance to the public. The research on public expectations regarding assistance from critical infrastructure operators was addressed in [3]. This under-researched problem was solved, based on the key issues that emerged as a result of a review of the literature on public expectations of transport infrastructure operators in disaster management. The results of an internet survey examining social sensitivity to disasters are presented. The results indicate that members of the public will expect that CI operators will contribute to responding in crisis situations, so as to provide means of evacuation and assistance in time-consuming reconstruction. Recommendations were made on how CI operators can meet these expectations. Fig. 3 shows from which services the respondents expect help after the disaster. Over 90% of respondents chose firefighters and first aid rescuers, and over 80% - police and crisis management personnel. CI operators are the next most frequently chosen ones, 73% of respondents expect to provide assistance. It seems that expectations are slightly lower for volunteers (64%) and neighbours (57%). Only 1% of respondents stated that they did not expect any help. In general, the survey showed that 96% of respondents agree or strongly agree that CI operators should provide means to evacuate the local population (Figure 3).
There was no significant difference of opinion among the respondents on the basis of sex, age, education level, nationality or experience resulting from previous disasters. When asked whether respondents expect CI operators to help in their long-term rebuilding, 75% agreed or strongly agreed (Figure 5). Differences of opinion were observed between residents of different countries. Respondents in Portugal have much higher expectations than others that CI operators will be helping them for a longer period, 92% agree or strongly agree with such a requirement. The respondents in Norway least expect help from CI operators - only 51% are of the opinion, and they do not agree or strongly disagree with 16% (compared to 7% or less in the case of the second surveyed nationality). Respondents who experienced earlier disasters have lower expectations of assistance from CI operators (68%) than those who did not have previous experience (78%).

![Fig. 3 Expectations regarding disaster relief](3)

![Fig. 4 Expectations regarding the provision of evacuation measures by CI operators](3)
The increase in public exposure to natural disasters in relation to observed climate changes has been highlighted in the publication [2] for at least the last 10 years. It was emphasized that the perception of the gap in the protection of society against natural disasters, also by the leaders of the public and private sectors, is still weak. Therefore, the first step towards increasing the authorities’ interest in vulnerability is to assess the expected number of future natural disasters and their consequences. The paper [2] presents a relatively simple methodology of approach to this problem - it is proposed to anticipate the expected number of natural disasters based on the Crow AMSSA model and to assess the gap based on the Bow Tie analysis (Figure 6). Criteria of vulnerability were also proposed as a reference point for supporting decision-making regarding the need to limit their vulnerability to natural disasters.

**Fig. 5** Expectations regarding long-term help [3]

**Fig. 6** Scheme of vulnerability analysis method Bow Tie [2]
An exemplary analysis was made for the effects of disastrous rainfall in the Rio de Janeiro area. One of the estimated parameters of the method is the average time between threats - storms - Fig. 7. Over the next five years, the expected number of catastrophic rainfall is 1.7.

![Fig. 7 Trend of mean time between storms [2]](image)

The scheme of the vulnerability model is shown in Fig. 8. Then the vulnerability rate is evaluated as the product [K]:

\[
\text{Vulnerability} = \text{ENHS} \times \text{CM1} \times \text{CM2} \times \text{Co1} \times \text{END}
\]

![Fig. 8 Susceptibility to strong rain [2]](image)

The estimated values of the Bow Tie elements (Figure 8) are:
- potential causes (exposure): strong storm \( \text{ENHS} = 1.0 \);
- control measures 1: monitoring and weather alarm \( \text{CM1} = 100\% \);
- control measures 2: CM2 population reallocation = 100%;
- loss of control (vulnerability): the probability of heavy rain affects Rio de Janeiro city = 100%;
- corrective actions (coping capacity): emergency response \( \text{Co1} = 100\% \);
- consequences: deaths - at least 1, \( \text{END} = 1 \).
It was emphasized [2] the importance of understanding why control measures and coping capacity were estimated at 100% of failures in the last 10 years. When it comes to weather forecasting and alarming, they were not effective due to outdated weather forecasting technologies in Rio de Janeiro, as well as the ineffectiveness of alerting the population. If the storm is reliably detected on time, it is not possible to move the population to a safe area because there is not enough free space for 1.5 million people who live in vulnerable areas in Favelas in the state of Rio de Janeiro. In addition, the majority of people are afraid that they will not be able to return to their homes after the natural disaster. Regarding the efficiency of coping, it is considered [2] that lowering the level of sensitivity resulting in only one death will be an unacceptable level. The effectiveness of emergency services during the rescue operation is insufficient; they do not have enough resources. Even considering the lowest possible number of deaths, the vulnerability is still unacceptable.

The 53th ESReDA seminar [7] focused on the issues of foresight challenges (predictions) in increasing security. 25 presentations were divided into 9 sessions concerning, among others problems of transferring foresight methods to the area of security. The introductory lecture discussed the problem of using foresight as a tool in creating policy in the field of security management.

Conventional security management is based on approaches to prevention and protection, but especially after disasters that have occurred, it is not enough. Reactive post-event approaches are valuable strategies for providing information and lessons on deficiencies in risk management. Analysis of major accidents and crises has shown that early warning signs have emerged that could be observed and used as valuable information to design “appropriate tools” and proactive strategies to prevent major events. Such lost opportunities indicate the need to improve foresight methods to improve safety management.

Several sectors of advanced technologies, such as aviation and nuclear energy, have achieved a high level of efficiency. Their call for next generation safety strategies and more proactive approaches has expanded to other sectors over the last decades. The transition from the approach to safety management, in which the improvement is based mainly on the observed facts for the use of foresight methods, requires overcoming many obstacles of a both theoretical and practical nature, such as:

- How to strengthen the human imagination in the area of security: can we go beyond the approach and scenario techniques?
- How can forensic theories, methods and techniques contribute to a broad risk assessment to improve systematic and holistic security management?
- Dealing with short-term and long-term forecasting: what methods/approaches are more appropriate for both?
State of knowledge on reliability and safety in the light of the scientific conferences...
Stan wiedzy o niezawodności i bezpieczeństwie w świetle konferencji naukowych...

- How can we predict the new, multi-faceted threats posed by new technologies, the digital revolution, the 4.0 industry, etc.? What can you do to improve the management of emerging threats?
- How to detect and handle early warning signs (EWS), weak signals, accident precursors, etc.? Can the analysis techniques developed for 'big events' (accidents, critical situations) be applied to 'minor events' (EWS, weak signals) or are new classes of techniques needed?
- What anomalies/surprises should we pay attention to? How to distinguish between signal and noise? How to deal with and use information services?
- How to increase the visibility of EWS? Are there tools and methods available? If so, what are they?
- What is the role of leading indicators and can they help to achieve the effectiveness of foresight? If so, how?
- Are new methods and technologies related to 'large data' part of the solution?
- How does the social climate influence the risk awareness and the organization's ability to identify early warning signals (reporting culture, talking behaviour and psychological security, debate, bad news approach, etc.)?
- How can security analysts generate the political capital needed to trigger organizational change if they cannot point to an earlier accident to demonstrate the need to improve and face the cost challenge?
- Is the knowledge of the past outdated? Is the current practice of knowledge management and learning organization well organized to face security foresight?
- How can foresight improve immunity and prevent accidents?
- How have some sectors become highly reliable, ultra-secure, non-plus ultra-safe? Why are there so many differences (performance, approach) in all sectors?
- Are new methods and technologies linked to 'big data' as part of the solution?

3. Conclusions

Taking into account the numerous participation of conference participants, both from academic circles and people working in enterprises, it can be concluded that the subject of reliability and security, both in the cognitive and application aspects, is still developing effectively. In 2018, the continuation of existing projects is planned. The ESREL 2018 conference will take place on June 17-21, 2018 at the Norwegian University of Science and Technology in Trondheim, Norway. The 54th ESReDA seminar is scheduled for 24-26 April 2018 at the University of Nantes (France), and the 55th seminar will be held in Bucharest in October / November 2018. It is also worth paying attention to the EuroMaintenance 4.0 conference, organized by the European Federation of National Maintenance Society EFNMS (PNTTE is a member of this organization), which will take place on September 24-27, 2018 in Antwerp (Belgium).
Fig. 9 Security paradigms and SM approach to a nuclear power plant [6]

4. References


State of knowledge on reliability and safety in the light of the scientific conferences...
Stan wiedzy o niezawodności i bezpieczeństwie w świetle konferencji naukowych...


Assist. Prof. Dr Hab. Eng. Marek Młyńczak is graduated from Wrocław University of Science and Technology and currently is a member of research and teaching staff in that University in the Faculty of Mechanical Engineering, in the Chair of Maintenance and Operation of Logistics, Transportation and Hydraulic Systems. His field of interests cover methods of operational field testing as well as risk assessment in technical systems. He works on operation and maintenance of technical objects, reliability, degradation and diagnostics directed on failure prevention. He is a member of Committee of Machine Constriction of Polish Science Academy, Polish Scientific and Technical Society of Operation and Maintenance, Polish Society of Safety and Reliability (Share 50%).

Professor Tomasz Nowakowski, Wrocław University of Science and Technology, dean of Mechanical Engineering Faculty, head of Chair of Maintenance and Operation of Logistics, Transportation and Hydraulic Systems. Member of Transport Committee of Polish Academy of Science, vice-president of Polish Maintenance Society, chief editor of scientific journal “Logistics and Transport”. Chairman of Winter School on Reliability. Major fields of interest concern: reliability, maintainability, safety of technical (generally transportation and logistics) systems, computer aided operation, knowledge based (expert) systems, uncertainty of operation & maintenance data (Share 50%).