



# Cloud Decision Support System for Risk Management in Railway Transportation

Wojciech Górka<sup>1</sup>, Jacek Bagiński<sup>1</sup>, Michał Socha<sup>1</sup>, Tomasz Stęclik<sup>1</sup>, Dawid Leśniak<sup>2</sup>, Marek Wojtas<sup>2</sup>, Barbara Flisiuk<sup>1</sup><sup>a</sup> and Marcin Michalak<sup>1</sup><sup>b</sup>

<sup>1</sup>Research Network LUKASIEWICZ — Institute of Innovative Technologies EMAG,  
ul. Leopolda 31, 40-189 Katowice, Poland

<sup>2</sup>Telvis Sp. z o.o., ul. Karoliny 4, 40-189 Katowice, Poland

**Keywords:** Decision Support System, Safety Management System, Risk Management, Software Support, Cloud Server.

**Abstract:** The paper features the development of a decision support system for railway transportation based on risk management. The implementation of risk management in this area is required by EU and national regulations. At present, there are no dedicated systems that would provide complex support of this process and, at the same time, enable to exchange experience and develop a common knowledge base not only on the level of a particular railway company, but also the whole industry. The solution presented in this paper assists the personnel responsible for risk management, allows to use a knowledge base and expertise, and supports data exchange between particular organizations on the railway market.

## 1 INTRODUCTION

The risk management process is carried out in an organization by its managers and employees. It is reflected in the organization's strategy and covers the whole organization. The goal of risk management is to identify events, or potential events, which could impact the fulfilment of the organization's objectives and to keep the risk on an accepted level.

Each organization is vulnerable to certain risks which might seriously disrupt its functioning. Railway transportation is particularly important in this respect because it is a part of the national critical infrastructure. Having this in mind and realizing the benefits stemming from risk management, such as lower maintenance cost due to deeper awareness of events and security incidents, preparedness for crisis situations, and selection of security measures adequate to potential losses, it is obvious to recognize risk management as an indispensable process in railway transportation companies (a case study of traction break due to icing and description of a decision making process are provided in (Bagiński et al., 2019)).

This requirement results not only from the desire to improve security and reduce the frequency and con-


sequences of events, but also from legal regulations imposed by national-level authorities (e.g. in Poland (Ministry of Infrastructure and Development, 2015)) and EU-level institutions (e.g. (European Commission, 2012)). Currently, there are several standards where expert knowledge on risk management is collected (Rausand, 2011).


The issues of risk management can be considered in terms of making decisions which are appropriate for the sake of the current environmental conditions of the process and for the sake of expected future state of the process.

Decision support systems (DSS) have been applied more and more often in different areas of human activity. The DSSes — depending on the areas and purposes of their application — make use of artificial intelligence methods, knowledge engineering, multi-criteria analysis, operational research, and decision theory.

Although there are known supporting systems for public urban transport (Bellini et al., 2017) such solutions cannot be applied directly in rail transport. It is mostly due to the fact that rail transportation is much more restricted: it is more difficult to get the permission for rail transportation, there are fewer carriers and other companies, the rail traffic is more regular and scheduled (similarly to air traffic).

So, in the railway industry, there are currently no

<sup>a</sup> <https://orcid.org/0000-0002-0106-591X>

<sup>b</sup> <https://orcid.org/0000-0001-9979-8208>

systems that would allow continuous exchange of information on safety and security (e.g. information regarding threats, existing vulnerabilities). According to national legal requirements, stakeholders of the Polish railway system (railway companies, infrastructure managers, entities responsible for maintenance) are obliged to immediately report accidents, serious accidents and incidents to the National Railway Accident Investigation Commission and the national Office of Rail Transport (ORT).

The lack of any DSS dedicated to risk management in the railway transportation branch was one of the motivations to launch the project called Central Threat Register (CTR): The management system of information and expertise knowledge about threats for railway transportation safety.

In the paper the selected elements and aspects of developed CTR system are presented. They focus on the risk management processes, cloud architecture of the system, problems of data sharing and anonymization. The necessity of such system development came straight from rail companies. CTR is designed as a cloud system, which comes from the business model of its selling and licensing (see Section 5.1). Moreover, such an architecture improves data collecting and sharing as well as performing statistical and risk analyses.

The CRT system is dedicated to support security representatives work in railway transport companies, support activities in risk management, provision of transport services and rail infrastructure maintenance. Moreover, the risk analysis module and decision support module are more generic and may be used in different branches of industry too.

The system is still in the development phase, in which rail transportation experts participate. During this phase real accidents and threats cases are analyzed.

The paper is organized as follows: it starts from a description of the results of a questionnaire conducted amongst 24 Polish railway companies; afterwards, a short description of related works in the areas of risk management and DSS systems is presented; the following section brings results of some preliminary studies in the CTR system requirements; next section presents the selected elements of the system architecture and is followed by a presentation of two of the most important CTR system use cases; the paper ends with some conclusions and perspectives of further works and the system development.

## 2 RISK MANAGEMENT AND DECISION SUPPORT IN POLISH RAILWAY TRANSPORTATION

Risk management is a relatively new and open issue in Polish railway transportation: the appropriate Polish standard comes from 2018 (Polish Committee for Standardization, 2018). As an element of risk management, railway transportation authorities require new fact sheets, reports and summary information reports (e.g. published by ORT). Moreover, railway companies do not exchange information about threats, though they unanimously declare they would be willing to use such data.

To better understand different approaches to risk management performing, the authors conducted a questionnaire among safety managers from 24 Polish railway companies. Almost 80% of those questioned said they did not use any IT systems supporting risk management, security management (SMS — Security Management System) or maintenance (MMS — Maintenance Management System). Only 4 respondents admitted they used IT management support systems. Most respondents used basic commonly available programs to maintain threats and events registers and to prepare reports, i.e. text editors and spreadsheets. Alternatively, these documents were produced as paper ones. Fewer than 30% of those questioned used IT systems to support the collection and analysis of information about events. Only 2 respondents declared they used IT support systems to exchange information about the occurring events and threats. Over 90% of the respondents admitted they had not used any systems supporting mutual information exchange and 100% of them were willing to apply a system for anonymous exchange of information, should such a system be developed.

The above shows that the current level of information exchange is not enough. This results from the lack of knowledge, including the lack of awareness about benefits coming from risk management and possibility to get prepared for the threats before they actually occur. Now most corrective actions and analyses are made no sooner than after the event occurs or as a result of the event. Moreover, there are only few available risk management support tools dedicated to particular industries or infrastructures. The existing tools do not support information exchange or use of data from the whole industry or infrastructure.

### 3 RELATED WORKS

In this section a short overview of the present approaches to risk management and existing applications of DSS will be presented.

#### 3.1 Risk Management

There are a number of solutions on the Polish market which offer risk management support for railway transportation, e.g. RailSoft (Petrosoft, 2017). The RailSoft software is an integrated security management system for railway companies in accordance with the requirements of MMS/SMS. The software has an analysis module RAMS (Reliability, Availability, Maintainability, Safety) which enables to test railway systems in terms of their reliability, maintenance and application safety. RailSoft also allows to generate reports about security events in the company, which can be sent to the national ORT. Still, the system does not ensure the exchange of information about security events between railway companies.

There are also applications for risk analysis and assessment, though these solutions are not dedicated to railway companies. The available software was designed to assess the risk for classified information, occupational hazards and operational risk. For example, the application Risk Analysis (F-tec, 2019) enables to analyze classified information in accordance with the requirements of the Internal Security Agency.

There is no obligation to immediately inform about identified internal threats or vulnerabilities. ORT provides a portal where people can report detected threats, security issues. However, in practice, even if railway companies report such information, usually they do not do it on a regular basis. There are more elaborate tools supporting analyses, e.g. Reliability Workbench (Isograph, 2019), but they do not offer the threat information exchange option.

Basically, on the European market there are no integrated systems or platforms for the management of railway threats, yet there have been attempts to develop and implement such platforms. For example, European Railway Agency (ERA) launched the Safety Alerts IT Tool (SAIT) platform to exchange information about events that can potentially lead to accidents. The obligation to exchange such information is a new requirement imposed by a European directive (European Parliament, 2016). ERA facilitates one more application, ERA SMS, which enables carriers and managers to assess the functioning of their security management systems. The application allows to check the conformance with new SMS requirements (so called 4th Railway Package).

#### 3.2 Decision Support Systems

Decision support systems have evolved with the development of technology (Shim et al., 2002) and as it was mentioned in the Introduction section, there are several types of DSSes defined in literature (Power et al., 2015), such as: data-driven, model-driven, document-driven, communication-driven, and knowledge-driven DSS. A decision support system can be of one type, however, it can also contain subsystems representing different DSS types.

A characteristic feature of a data-driven DSS is access to and processing of time series that can be internal or external company data (Power, 2008). The data that are processed within the system can be stored in various locations starting from a file system, where a query and retrieval functionality is provided, up to a data warehouse (Kimball and Ross, 2011; Poe et al., 1997), where advanced data manipulation methods are available. An appropriate data repository is particularly important for further analysis, inference and decision support. Thanks to that, it is possible to integrate data from various sources and to clean and prepare them. Such data-driven systems are used for data originating, e.g., from sensors (Dong et al., 2018; Ślęzak et al., 2018; Janusz et al., 2017).

The data stored in a system repository can be processed by means of advanced data analysis methods in order to derive a model assisting in decision making. The systems where a model plays central role are called model-driven DSSes (Power and Sharda, 2007). Such systems enable a non-technical user to access a model by a dedicated interface. Additionally, the created model is intended to be applied repeatedly in the same or similar decision situation. The models utilized in the system can be of various types, e.g., differential equation models, analytical hierarchy process based models, or forecasting models.

### 4 PRELIMINARY STUDIES

The support of risk management has to comprise supporting tools (which implement certain knowable practices), e.g. risk analysis methods, risk analyzers, vulnerability analyzers, countermeasures. The support must be based on credible data on whose basis (having already concrete quantitative data) it is possible to recommend certain solutions or to assess the importance of defined threats. The data necessary for risk analyses cover a wide spectrum of information, in terms of range, structure, granulation, and quantitative aspects. A part of the data which are the basis to conduct risk analyses are entered by the opera-

tors of domain systems, a part come from online automatic sensors, and another part are secondary data, i.e. results of partial analyses. Thus, it is necessary for the system to acquire information about events (accidents, incidents, failures of railway stock, equipment, etc). The acquisition of these data will give access to the statistics about the occurrence of certain phenomena within the organization. This, in turn, allows to follow the trends of identified risks. In addition, the acquisition of data about events makes it possible to examine the causes of certain phenomena and points to interim methods to solve them. Finally, it is possible to reason about the efficiency of the applied solutions to mitigate the consequences of the events or to reduce their frequency. The causes, actions, threats, and consequences are elements used in the analytical part.

Apart from quantitative data (based on events in the company) it is necessary, particularly during the first stage of the system work, to support the users with expert knowledge. This can be done by providing contact with a security expert. The users should be able to contact the experts directly. Direct communication in the system will come down to running an experts base and defining the range of their competence. Expert knowledge is not only the support from experts while solving current problems but also the knowledge saved and available in the system.

Among the prerequisites identified during preliminary analyses of the system design there is an assumption that the system should have a modular structure. Thanks to that it will be possible to use a part of the developed system in other risk management systems dedicated to domains other than railway transportation. The development of a domain system only for one sector (railway transport) would raise the cost of an individual IT system. This led to the development of a modular system whose components can be used to construct systems dedicated to other industrial sectors. Though the PN-ISO 31000 (Polish Committee for Standardization, 2018) standard remains the basis of the system, the specifics of particular sectors (e.g. railway, telecommunications, finances, fuels, road transport) suggest that making a universal system for all domains would not be a good solution. Thus the common part of the system will cover certain definitions of data structures, algorithms implementation, program libraries, and editors (tools) supporting knowledge acquisition.

All these assumptions and requirements laid down the basis to carry out the requirements analysis and the functional analysis of the system.

## 5 CLOUD DSS FOR RISK MANAGEMENT IN RAILWAY TRANSPORT

In the first stage of the system design the project team focused on a data schema that would be general enough to become a kind of a common point for risk management systems. Such a universal data structure allows not only to develop domain systems on the basis of the same data structure, but also to exchange certain data elements between particular instances of the system (this is important in the case of cloud solutions). The first step was to systematize the terms used in the system and to determine the context of their use in particular parts of the system (Figure 1).

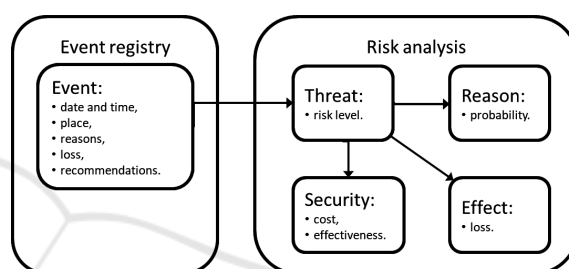


Figure 1: Dependencies and data flow in the system.

In risk management there are four basic terms: threat, vulnerability (cause), consequence, and preventive action (security measure). Their mutual relations can be seen in Figure 1. In addition, risk management covers the assessment of the current situation. Therefore the system should store the events that would make the basis for the analyses. An event will be assigned to an existing threat. The statistics of the event occurrence can be used for the assessment of threats, probability and potential consequences of the threat materialization.

### 5.1 System Architecture

The system architecture should allow for easy access to the system, data exchange between particular companies of the railway sector and mechanisms enabling to preserve and promote expert knowledge in the system. The best and the most commonly used method is to develop the system in a cloud as it is presented in Figure 2.

Such a solution facilitates the system commercialization, particularly when it comes to smaller companies of the railway sector: it is possible to adapt the price to the client's financial abilities, reduce maintenance cost, eliminate the necessity to install the system, and provide online update (Avram, 2014). Another argument is that the exchange of data between



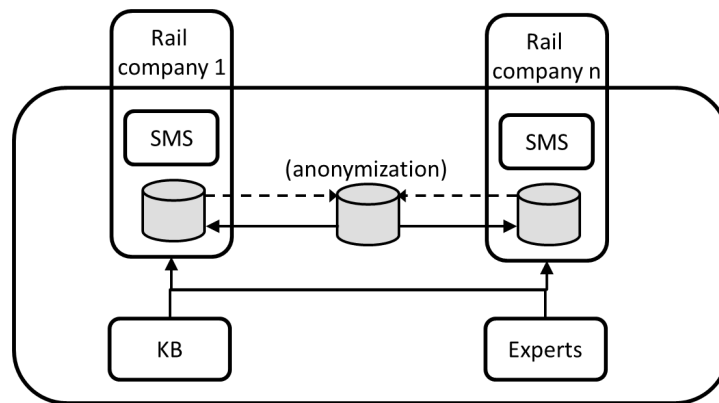


Figure 2: System architecture.

particular users is easier. It is not necessary to make complicated integration of systems, either between each other or with the central node – all data are stored in one point and it is easy to use them, provided that the given company gives consent to that. The access to the system will be provided by a browser – the system interface will have a WEB form.

The revision of existing practices and interviews with the personnel responsible for keeping records of risk management events showed that the events collection and risk analysis were strictly related to each other. Frequently, the information belonging to the event description, e.g. consequences, causes or prevention actions, was treated already as a resulting element of risk analysis. In the developed system it was proposed to separate these two areas. Thus the system is logically divided into the supervision part related to the collection of events and the analytical part where, based on these events, threats are defined and risk indicators calculated.

An important element of the system architecture is the method of defining the knowledge base. The system will have an independent data structure where the patterns of threats, security controls, vulnerabilities, and consequences will be stored. These data will be constantly updated by the system experts based on their experiences and observations. The users who will define their own risk-related elements (threats, security controls, etc) will refer to the patterns from the knowledge base – the patterns will be given as original elements for users-defined elements.

This solution will allow to acquire global information for the whole system, generate charts and statistics based on data from the whole sector. If, defining their own new threats, the users refer to a threat from the knowledge base, the information or data about this threat described by one user can be used as hints for other users who refer to this element too. This aspect of the system is presented in Figure 3.

## 5.2 Data Anonymization

The system architecture facilitates and promotes mutual use of data by particular stakeholders of the railway market who will make use of the developed system. As it was mentioned before, this situation evokes certain concern about possible disclosure of business secrets. Therefore it is necessary to anonymize the data, so that only this information could be provided which does not subject the user to unauthorized disclosure of confidential data or business secrets. To anonymize the data, it is possible to use generalization or permutation (Cormode and Srivastava, 2010) as well as, in certain cases, clustering-based or graph modification approaches (Zhou et al., 2008). The developed system adopts data generalization with the use of the knowledge base. Thus the anonymization is reflected in the system architecture and in the data model employed in the system. First of all, it was decided to exchange aggregated quantitative data. For example, it would be possible to get access to collective data about the number of occurrences of the given type of events (translated into certain threats) but not to the contents of the events as such. Certain collective data will be collected for knowledge base elements and the related elements defined by the users. The technique of using the knowledge base as an intermediary between data of different organizations guarantees that the anonymization will be applied.

## 6 SAMPLE USE CASES

In this subsection two use cases are presented. They reflect one of the most important situations: the first one represents a single risk analysis and the second one illustrates data flow in data analyzing, anonymization and sharing.

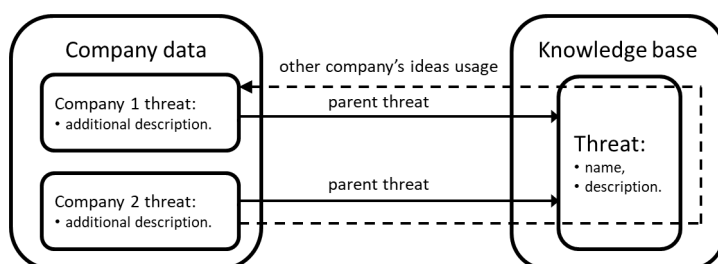


Figure 3: Use of knowledge base.

The first use case deals with the single risk analysis performance. The threat analysis will comprise, in fact, several analyses. It will contain not only a risk analysis for a certain threat but also the identification of the threat causes and consequences as well as possible security measures. Different types of analyses will support these operations. For the given threat the final risk level will be determined with the use of one of available analyses, e.g. FMEA.

A threat analysis, conducted by a railway company employee responsible for analyses, is done with the use of available resources, such as the catalogues of previously collected data: consequences, security measures, causes. For the purpose of the analysis the user will have access to events associated with the threat, so that, based on their descriptions (including: recommendations of the commission, quantitative consequences – victims, delays, losses) he/she can draw proper conclusions and define suitable causes, consequences and security measures.

An expert analysis, in turn, will be ordered by the company’s representatives. Here the expert can be an employee of a railway company, ORT or other institution. He/she must be familiar with the railway transport specifics and have enough expert knowledge in this domain. The expert will receive an order with the description resulting from already analyzed data. The description will have a form of a text paraphrase of the collected data (from threat analysis), so the expert will not have direct access to threat-related data (causes, security measures, consequences) but will be provided with their text version.

Based on the description, the expert will be able to examine the issue. The result of his/her work will be either a description with remarks or his/her own analyses. It will be possible for the expert to get familiar with the company’s own analyses in the form of documents from analyzers.

The actors of the use case (security representative and security expert) and the whole use case are presented in Figure 4.

The second use case deals with the data analysis and sharing. A railway company employee who is re-

sponsible for security initiates the process of providing information about new threats, security measures, etc. At this stage he/she decides which information should be released to the remaining users of CTR. The provided data are anonymized in the next stage.

The second actor of the process is the system administrator whose task is to approve the anonymized data provided by the employees of particular railway companies. This step allows to ensure coherence and suitable quality of data to be stored in the common data base. The process itself is finalized by supplementing particular catalogues of the database.

The scheme of the use case is presented in Figure 5.

## 7 CONCLUSIONS AND FURTHER WORKS

In the paper the new developed decision support system for risk management in Polish railway transportation is presented. The description consists of an overview of most general aspects such as data anonymization, data sharing, experts involvement, decision support, and cloud architecture.

Big railway transportation companies, which took part in the above mentioned questionnaire, have at their disposal some tools supporting risk analyses. Still, these are local-level solutions. Therefore the project is not focused on the risk analysis as such but on collecting information from the whole railway transport domain (e.g. information how often security incidents occur, etc). The risk analysis module is extra support for smaller railway transportation companies which have not used such tools so far. The AHP-based decision support module, in turn, is an added value for this domain as this method has not been employed by railway carriers before.

The presented ideas for the system development are implemented progressively within the project. Not until the implementation stage has been concluded, the system use by real users will allow to assess whether the decisions about possible solutions were

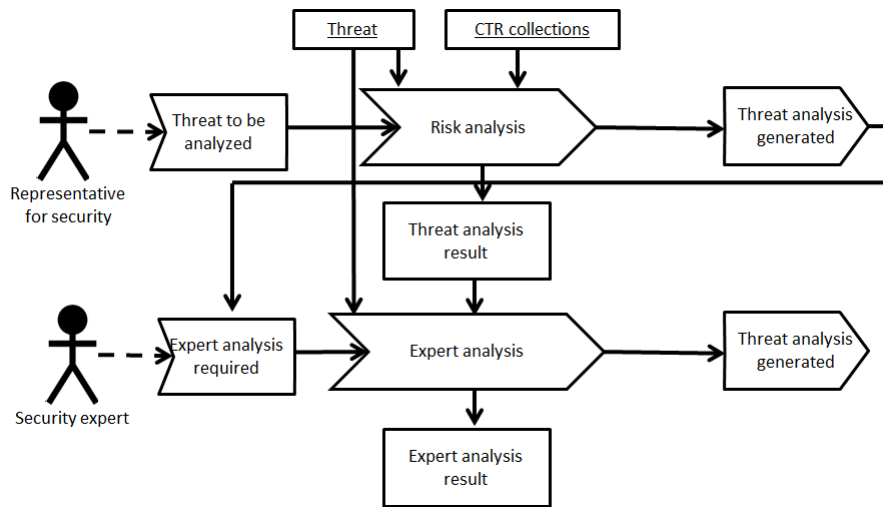


Figure 4: The use case illustrating the single risk analysis.

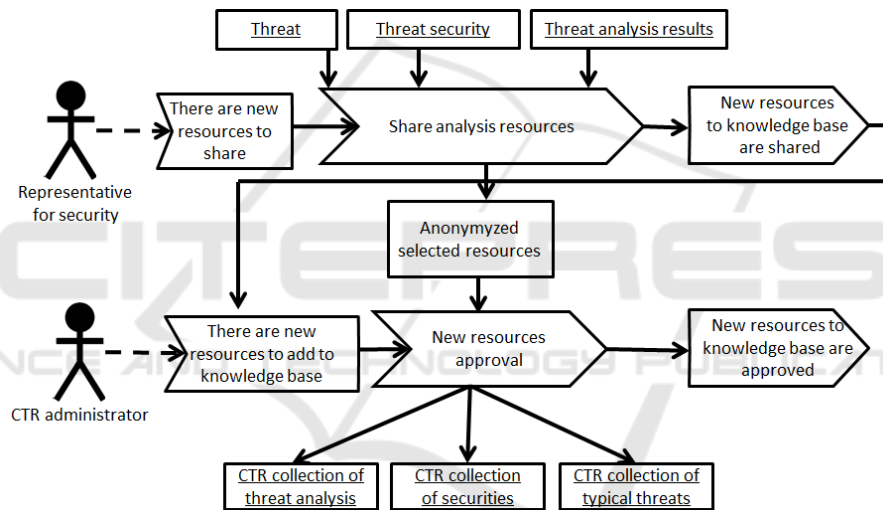


Figure 5: The use case illustrating the single data analysis and sharing.

right. The system is built in the Agile methodology, so that permanent contacts with domain experts could allow to verify the correctness of successive system sections. A threat to proper functioning of the system may be the users' lack of willingness to exchange data between each other (in spite of the existing data anonymization). A supporting action here will be a system of incentives, i.e. if a user wants to access data from other users, he/she has to give access to his/her data in return.

An important element that will impact the success of the system will be its status during the start-up — whether the system already has some data, which are an added value, in the form of domain knowledge. Thus, the contents of the data base should be prepared by the domain experts already at the stage of the system implementation. This will be done by means of a

special interface for knowledge base editing.

The developed common part for different risk management systems in the organization will be verified by an attempt to apply it in a different sector. No doubt, this will involve some changes or will require to work out another common elements. It is considered to give public access to this part of the system in the form of a framework for risk management systems.

On the basis of the feedback from the domain experts the modules of Knowledge Base and Experts are now filled with data. In addition, the companies' databases and the global anonymized database are filled with the sample initial data. The most important part of the project — the implementation in selected rail companies — is still ahead.

Our future works will also focus on the system

effectiveness and efficiency. Although the potential number of system users might not be high (the access to the rail transportation market is strictly supervised and the total number of companies does not exceed one hundred and several dozen) the next implementation phase may require to overcome some difficulties in the system operation.

## ACKNOWLEDGEMENTS

This work was supported by Polish National Centre for Research and Development (NCBiR) within the Operational Programme Intelligent Development: Grant No. POIR.04.01.02-00-0024/17-00 (Central Threat Register — The management system of information and expertise knowledge about threats for railway transportation safety).

## REFERENCES

- Avram, M. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, 12:529 – 534.
- Bagiński, J., Flisiuk, B., Górka, W., Rogowski, D., and Stęclik, T. (2019). Multi-criteria decision analysis in the railway risk management process. *Communications in Computer and Information Science*, 1018:126–138.
- Bellini, E., Ceravolo, P., and Nesi, P. (2017). Quantify resilience enhancement of uts through exploiting connected community and internet of everything emerging technologies. *ACM Trans. Internet Technol.*, 18(1):7:1–7:34.
- Cormode, G. and Srivastava, D. (2010). Anonymized data: Generation, models, usage. In *2010 IEEE 26th International Conference on Data Engineering (ICDE 2010)*, pages 1211–1212.
- Dong, F., Zhang, G., Lu, J., and Li, K. (2018). Fuzzy competence model drift detection for data-driven decision support systems. *Knowledge-Based Systems*, 143:284 – 294.
- European Commission (2012). Commission regulation no 1078/2012.
- European Parliament (2016). Directive 2016/798 on railway safety.
- F-tec (2019). <https://f-tec.pl/analiza-ryzyka/>.
- Isograph (2019). <https://www.isograph.com/software/reliability-workbench/>.
- Janusz, A., Grzegorowski, M., Michalak, M., Wróbel, L., Sikora, M., and Ślęzak, D. (2017). Predicting seismic events in coal mines based on underground sensor measurements. *Engineering Applications of Artificial Intelligence*, 64:83 – 94.
- Kimball, R. and Ross, M. (2011). *The data warehouse toolkit: the complete guide to dimensional modeling*. John Wiley & Sons.
- Ministry of Infrastructure and Development (2015). Common security indices decree. *Dziennik Ustaw*, 1061.
- Petrosoft (2017). <https://petrosoft.pl/produkty/oprogramowanie-kolejowe/>.
- Poe, V., Brobst, S., and Klauer, P. (1997). *Building a data warehouse for decision support*. Prentice-Hall, Inc.
- Polish Committee for Standardization (2018). Polish standard PN-ISO 31000:2018–08: Risk management — guidelines.
- Power, D. J. (2008). Understanding data-driven decision support systems. *Information Systems Management*, 25(2):149–154.
- Power, D. J. and Sharda, R. (2007). Model-driven decision support systems: Concepts and research directions. *Decision Support Systems*, 43(3):1044–1061.
- Power, D. J., Sharda, R., and Frada, B. (2015). *Decision Support Systems*, pages 1–4. American Cancer Society.
- Rausand, M. (2011). *Risk Assessment: Theory, Methods, and Applications*. Wiley.
- Shim, J. P., Warkentin, M., Courtney, J. F., Power, D. J., Sharda, R., and Carlsson, C. (2002). Past, present, and future of decision support technology. *Decision support systems*, 33(2):111–126.
- Ślęzak, D., Grzegorowski, M., Janusz, A., Kozielski, M., Nguyen, S. H., Sikora, M., Stawicki, S., and Wróbel, L. (2018). A framework for learning and embedding multi-sensor forecasting models into a decision support system: A case study of methane concentration in coal mines. *Information Sciences*, 451-452:112 – 133.
- Zhou, B., Pei, J., and Luk, W. (2008). A brief survey on anonymization techniques for privacy preserving publishing of social network data. *ACM SIGKDD Explorations Newsletter*, 10(2):12 – 22.