Advances in Science and Technology
Research Journal

Advances in Science and Technology Research Journal 2023, 17(2), 215–225
https://doi.org/10.12913/22998624/162188
ISSN 2299–8624, License CC-BY 4.0

Received: 2023.02.16
Accepted: 2023.03.15
Published: 2023.04.01

Mathematical and Technical Quantitative Methods for Risk Assessment in Public Crisis Management

Marek Kisilowski[1]

[1] Faculty of Management, Warsaw University of Technology, pl. Politechniki 1, 00-661 Warsaw, Poland
e-mail: Marek.Kisilowski@pw.edu.pl

ABSTRACT

The article shows that in crisis management, risks can be effectively analysed and managed by rational use of mathematical and technical methods. It presents two quantitative methods for risk assessment and a procedure for transferring the results to logistical social networks (LSNs). The need to use social logistical networks, where modern techniques can be applied, including the Internet of Things (IoT) or Machine-to-Machine (M2M) communication, enabling the collection of any amount of data to logistical social networks, is indicated. The article stresses that research on public crisis management must be interdisciplinary in nature, taking into account all aspects of security management, including social, technical and economic issues. Modern methods of assessing the state and risk of a crisis situation of individual elements of the systems generate an increasing number of data, the collection, collection, processing and sharing of which requires ensuring information security and protecting the personal freedom of the individual.

Keywords: crisis management, risk assessment, logistical social networks

INTRODUCTION

Public crisis management should be understood as a triad of risk – security – response. It is based on the work of Rausand [19], the work of Kaplan [8], Kaplan and Garrick [9], and Setlak et al. [20] it can be assumed that risk is related to what may happen in the future. Safety is related to the prevention (ex-ante action) of risks that are manifestations of risk. Response is the mitigation of the effects of the fulfillment of risks and threats (ex-post actions) involving both the direct neutralisation of the effects and the restoration of the pre-disruption (crisis or incident). The aim of this article is to show that it is possible to analyse and manage risks by using mathematical methods rationally.

In order to define the principles of applying quantitative methods in public crisis management, it is necessary to refer to selected areas of mathematics and technology, e.g. sensitivity theory or elements of technical equipment diagnostics. These will form the basis for formulating specific tasks. Such considerations enable quantitative risk assessment and lead to a wider use of mathematical and technical methods for risk assessment in public crisis management.

QUANTITATIVE RISK ASSESSMENT METHODS

Quantitative risk assessment is a complex process whose stages depend on a number of elements. Two of them can be considered fundamental, i.e. the scope of the analysis and the complexity of the objects under investigation. In order to define the principles for the application of quantitative methods in public crisis management, it is necessary to adopt a number of mathematical and technical areas, e.g. sensitivity theories or elements of technical device diagnostics, which will form the basis for the formulation of specific tasks. Such considerations for quantitative risk assessment lead to the need to make greater use of mathematical and technical methods for risk assessment in public crisis management. The methods used to quantitatively assess the condition of the facilities under investigation, e.g. technical equipment or system. Many scientific papers on the subject refer to similar mathematical methods. At present, this issue is dealt with by at least a few centres in the world, which include many identical elements in their research.

The scope of this review of methodologies shall be the mathematical methods used at different stages of risk analysis. The basic ones are: stochastic processes, statistical methods, fuzzy sets, sensitivity analysis, Fokker Planck's equations, Lagranger's equations, graph theory elements and reliability theory elements. These methods are applied both statistically and dynamically and, in essence, lead to similar solutions, despite the different areas of risk. The end result is always a kind of answer to the question: what is the essence of a risk in terms of its possibility?

It should be stressed that in all the methods mentioned, it is always possible to formulate a final report which can be transmitted electronically to various types of networks, e.g. *Logistics Social Networks* (LSN), which gives the possibility of creating risk management systems at any level of the state structure. The essence of this is to obtain from a given analysis a signal quantifying the risk potential, its scale, intensity, etc.

The scientific and practical challenge is to build or indicate a model. With this mathematical model, on the basis of which a quantitative analysis of the risk assessment can be carried out, the following range of activities is usually carried out:

- formulation of a risk analysis programme,
- to define the structure and scope of the analysis,
- defining the risks of possible dangerous events,
- to determine the causes of each hazardous event,
- determining the frequency of occurrence of a dangerous event,
- to establish a sequence of dangerous events,
- to establish scenarios that may arise in a dangerous event,
- defining relevant and typical scenarios for possible accidents,
- to determine the consequences that will arise after each accident,
- determining the frequency of dangerous events,
- assessing the possibility of a dangerous event (based on the adopted mathematical methods),
- description of emerging risk images - formulation of mathematical models,
- preparation of a risk analysis - the final report - then in the form of signals that can be recorded in the LSN.

For such a defined area of operation it is possible to present an algorithm defining the input and output and a functional element between input and output. Such an algorithm is presented in Figure 1, with the diagram presented there taken from Marvin Rausand's work [19] and supplemented with actions binding the algorithm to LSN and personal experience. Comments on these steps may be presented separately.

In order to carry out a quantitative risk analysis it is necessary to have access to a wide range of data. Such analysis therefore requires the collection, analysis and storage of data on an appropriate number of critical events. Such data is collected by various types of institutions, e.g. in the USA – the Reliability Information Analysis Center (RIAC) or in Europe – the European Safety, Reliability and Data Association (ESReDA). Tasks in the field of data collection practically do not have a uniform structure, but are created for various types of areas, such as nuclear energy, aviation, rail transport and industry. In Europe, the scope of data collection is regulated by the European Union's Seveso III Directive [5], which obliges the collection of data in a specific format and directs it to national authorities and the ESReDA database.

Analyses of mathematical models provide an answer to the question of what technical parameters are necessary to carry out quantitative risk assessment. These models describe the system of functioning of technical systems. An important group of data is knowledge of previous incidents in the test system or similar systems.

For the system to function properly it is necessary to determine its reliability. Therefore, data on the frequency of damage to elements are collected. They should be collected and grouped in databases. They should also be linked to LSNs so that they can be used for systems of the same type, operating in networks. This also requires proper archiving with the possibility of access according to specific keys. Some such solutions exist, such as Offshore Reliability (OREDA) [18].

Information obtained from the analysis of quantitative risk assessments for public management should be addressed to the LSN. Such a task

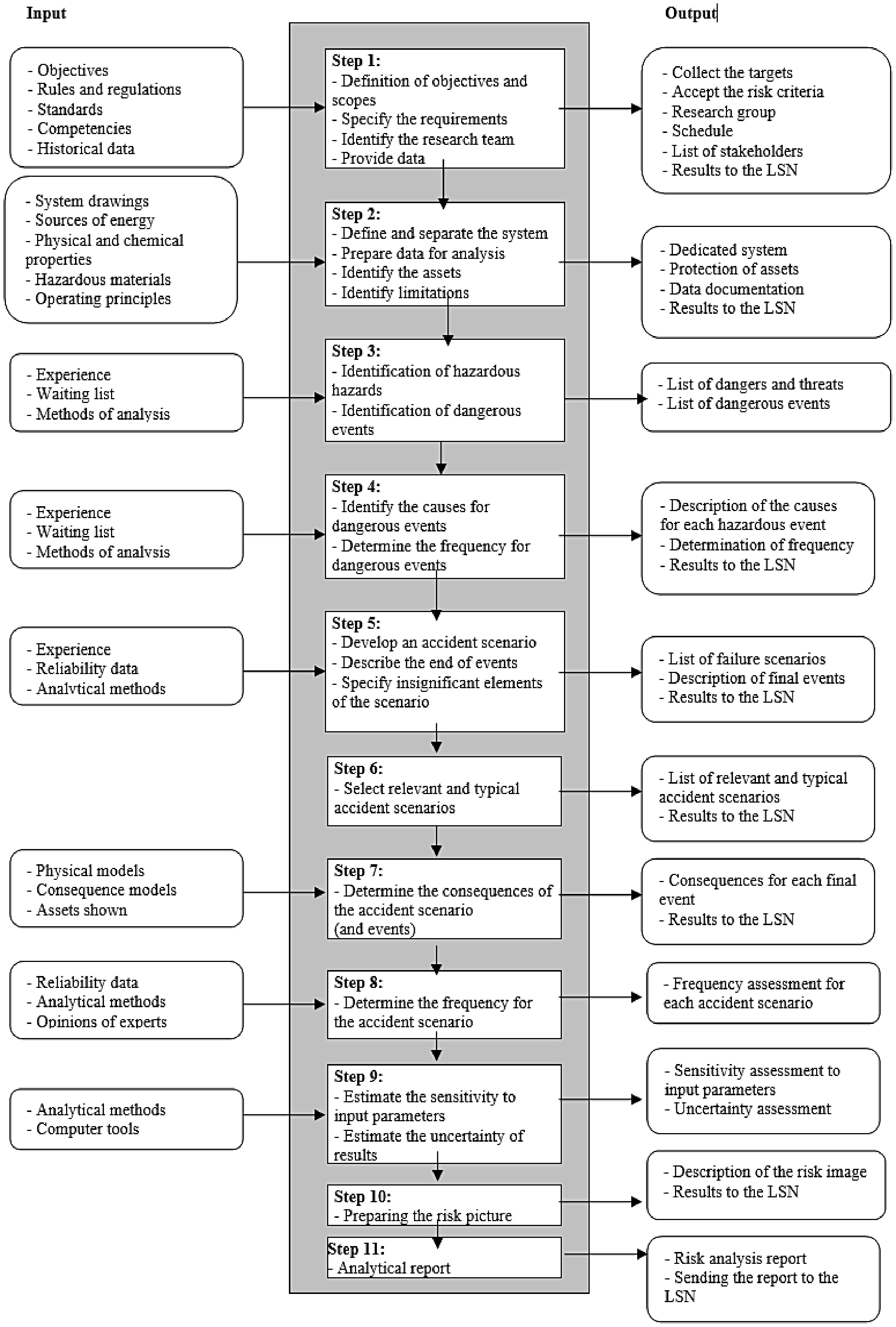
Input
Output
- Objectives
- Rules and regulations
- Standards
- Competencies
- Historical data
Step 1:
- Definition of objectives and scopes
- Specify the requirements
- Identify the research team
- Provide data
- Collect the targets
- Accept the risk criteria
- Research group
- Schedule
- List of stakeholders
- Results to the LSN
- System drawings
- Sources of energy
- Physical and chemical properties
- Hazardous materials
- Operating principles
Step 2:
- Define and separate the system
- Prepare data for analysis
- Identify the assets
- Identify limitations
- Dedicated system
- Protection of assets
- Data documentation
- Results to the LSN
- Experience
- Waiting list
- Methods of analysis
Step 3:
- Identification of hazardous hazards
- Identification of dangerous events
- List of dangers and threats
- List of dangerous events
- Experience
- Waiting list
- Methods of analysis
Step 4:
- Identify the causes for dangerous events
- Determine the frequency for dangerous events
- Description of the causes for each hazardous event
- Determination of frequency
- Results to the LSN
- Experience
- Reliability data
- Analytical methods
Step 5:
- Develop an accident scenario
- Describe the end of events
- Specify insignificant elements of the scenario
- List of failure scenarios
- Description of final events
- Results to the LSN
Step 6:
- Select relevant and typical accident scenarios
- List of relevant and typical accident scenarios
- Results to the LSN
- Physical models
- Consequence models
- Assets shown
Step 7:
- Determine the consequences of the accident scenario (and events)
- Consequences for each final event
- Results to the LSN
- Reliability data
- Analytical methods
- Opinions of experts
Step 8:
- Determine the frequency for the accident scenario
- Frequency assessment for each accident scenario
- Analytical methods
- Computer tools
Step 9:
- Estimate the sensitivity to input parameters
- Estimate the uncertainty of results
- Sensitivity assessment to input parameters
- Uncertainty assessment
Step 10:
- Preparing the risk picture
- Description of the risk image
- Results to the LSN
Step 11:
- Analytical report
- Risk analysis report
- Sending the report to the LSN

Fig. 1. Steps in risk analysis

can be briefly described. All information should reach the logistical social networks (LSNs). These networks make use of many modern technologies, e.g. in recent years the Internet of Things (IoT) has also been used for social logistical networks. One of the important works is the work by Atzori et al. [2], which shows the new architecture in the Social Internet of Things (SIoT). The Internet networks (Twitter, Facebook, Weibo, QQ) are used to study various elements of social life, including risk analysis. At the same time, IoT has become a strong tool for the transmission of digital logistical information, as shown in Figure 2.

A set of information flowing through the network may concern different areas, specific information may also concern quantitative elements of risk assessment. When considering IoT with regard to logistics, we have three problems to address. Firstly, there is the full integration of information throughout its transport route into the logistics network, which is extremely important for quantitative risk information. Secondly, there may be opportunities for behaviour to facilitate communication with organisations (in different networks), which makes it possible to signal emerging risks. Thirdly, the IoT can be used to collect data on logistical procedures also related to quantitative risk assessments.

A new paradigm in logistics networks is Machine to Machine (M2M), which is presented in the works of Ahmad et al. [1] and Mehmood et al. [16], which envisage the meeting of billions of intelligent communication devices with or without human beings, that is, communication machines. An important task that M2M fulfils in logistics is the problem of communication of the different types of information that are generated by M2M. The scope of this information is very wide and may also include information about the condition of the device, its reliability and the possibility of a threat to the operation of the device of the subject and the environment. The number of devices that can generate information can be very large and can include any range of information. This is important for processing information about the state of the risk; the machine, the factory and the environment. The amount of data on quantitative elements of risk assessment is relatively small (in relation to human communication), which leads to the possibility of carrying out optimisation processes ensuring good M2M performance in risk assessment. In the M2M network, an important device is the Relay Node *(*RN). The principles of operation of this system can be characterized by means of Figure 3.

The details of the system can be found in the work of Ahmad et al. [1]. The presented concept can be widely used to collect signals that characterize the state of the device or enterprise.

In order to verify the effectiveness of the M2M system, computer simulations were carried

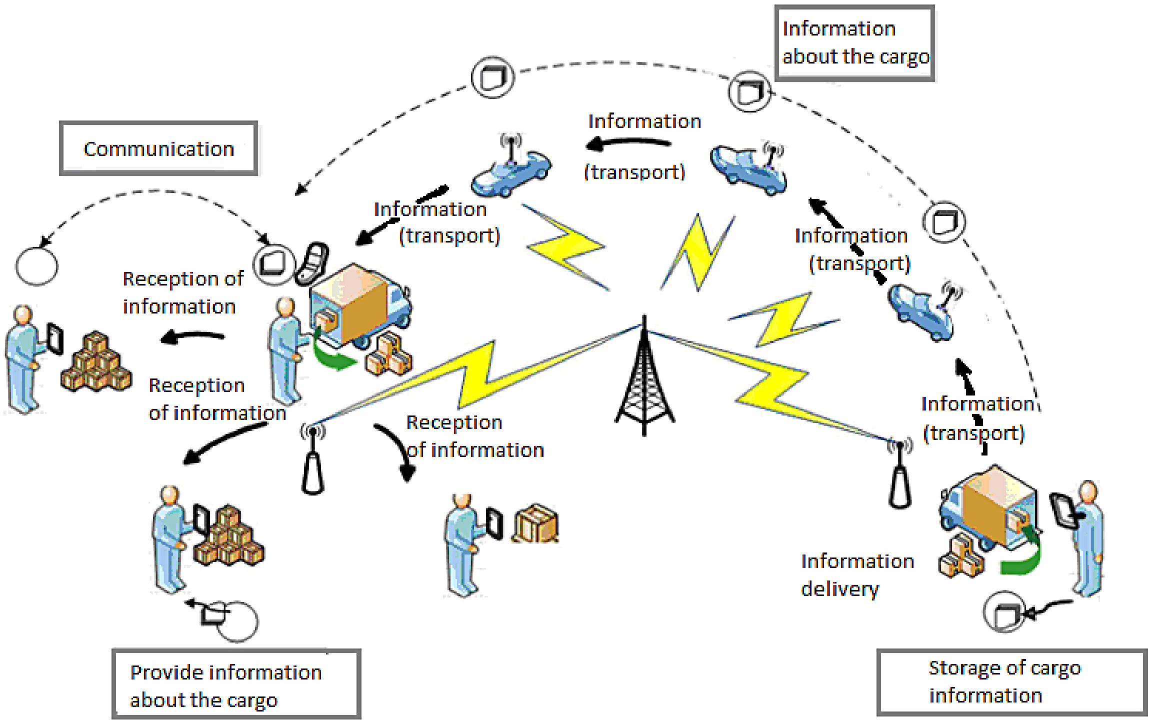

Fig. 2. Logistical information moving in the system

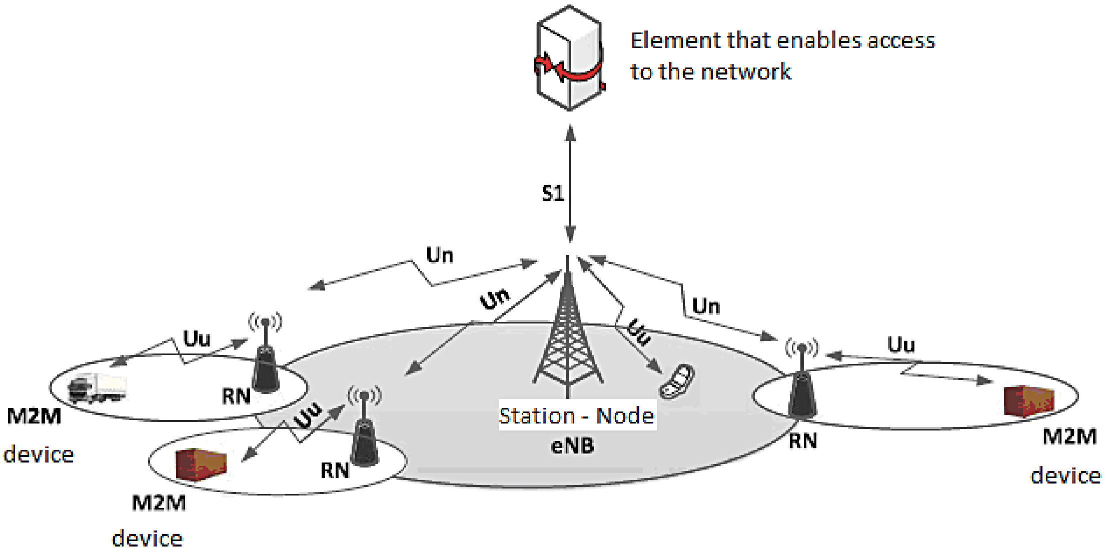

Fig. 3. M2M-LTE-A architecture with a relay node [1], where: eNB - Station - Node – access element, Uu – connection between M2M and RN, Un – connection between base station and RN.

out using various random event scenarios for a real public administration environment. This section presents an example of M2M traffic load in a crisis situation (e.g. earthquake, fire, terrorist attack, etc.). In such situations, in addition to the usual network traffic between the various components of the wireless network infrastructure (VoIP, Video Streaming, file transfer), there is additional M2M traffic. That is, additional traffic caused by the occurrence of a crisis event tries to enter the M2M wireless network. In conducting the scenario, the open source network models SimuLTE [20] , the number of M2M requests trying to access the LTE-A network at the same time in an interval of 1 second, was used. The settings of the SimuLTE scenario are listed in Table 1 [6]. In turn, the other parameters included in the M2M network are shown in Table 2.

The above scenario was simulated using the open-source SimuLTE network modeler in the OMNeT++ 4.6 environment, using the open-source INET Framework 2.3.0 modeling library [7]. The Matlab environment was used to visualize the results and define other components of the M2M system. Simulations were performed

Table 1. SimuLTE scenario settings

Parameter	Value
Simulation length	300 sec
Min. / max. (eNodeB-UE distance)	35 m / 300 m
Terminal velocity	120 km/h
Mobility model	Linear mobility
Transmission bandwidth	5 MHz (for Down-Link (DL) and Down-Link (UL) each)
No. of PRBs	25 (for DL and UL each)

Table 2. Parameters of M2M network components [6]

VoIP Model	Parameter	Setting
	1 Application packet	40 Bytes
	Interval	20 ms
	Lalkspnrts and silences	Default, settings
Video Streaming Model	Parameter	Setting
Video Streaming Model	Video size packet length	10 MB 1000 Bytes
	Frame interval	75 ms
M2M Model	Parameter	Setting
M2M Model	Packet size	128 Bytes
	Interval	1 sec
FTP Model	Parameter	Setting
	File size	20 MB

on two different computer platforms with different configurations. In all scenarios, the number of VoIP-UL, VoIP-DL, video streaming, File Transfer Protocol (FTP)-UL and FTP -L connections. Protocol (FTP)-UL and FTP-DL is 10 users each. The number of M2M increases until the M2M peak is reached, as shown in Table 3.

Exceeding the maximum number of M2M on the desktop computer (PC) platform, an error appears: "Error in module (TCP) of M2M server". Meanwhile, this error did not appear during simulation using the same parameters on the cluster platform. This result sheds light on the importance of platform resilience. Moreover, if we consider the results which show that the performance of voice users is unaffected by additional users, while file transfer and M2M traffic experience significant latency about four times higher. In addition, if we follow up on the content [15] in which the authors point out the maximum number of UEs that can overload an eNodeB, especially when multiple M2M devices are competing for network access in dense areas. Answers to the question of the maximum number of UEs could be as follows: 250 UEs, 320 UEs and 400 UEs.

The computer simulation results presented here show the concrete feasibility of M2M for a real-world government environment.

EXAMPLES OF MATHEMATICAL METHODS IN QUANTITATIVE RISK ASSESSMENT

Application of the sensitivity theory for risk assessment

Justifying the need to use mathematical methods in the quantitative assessment of risk, for example, two applications of mathematical methods can be shown. Marvin Rausand in his work [19] suggests using sensitivity analysis in the risk assessment process. These issues are similarly considered in the work of Kisilowski [12]. The problem posed can be solved based on the analysis of a mathematical model describing a technical object. The following assumptions

Table 3.

M2M traffic	16 B/1 sec	128 B/1 sec	6 KB/1 sec
Cluster platform	above 1000	above 1000	above 1000
PC platform	800	600	800

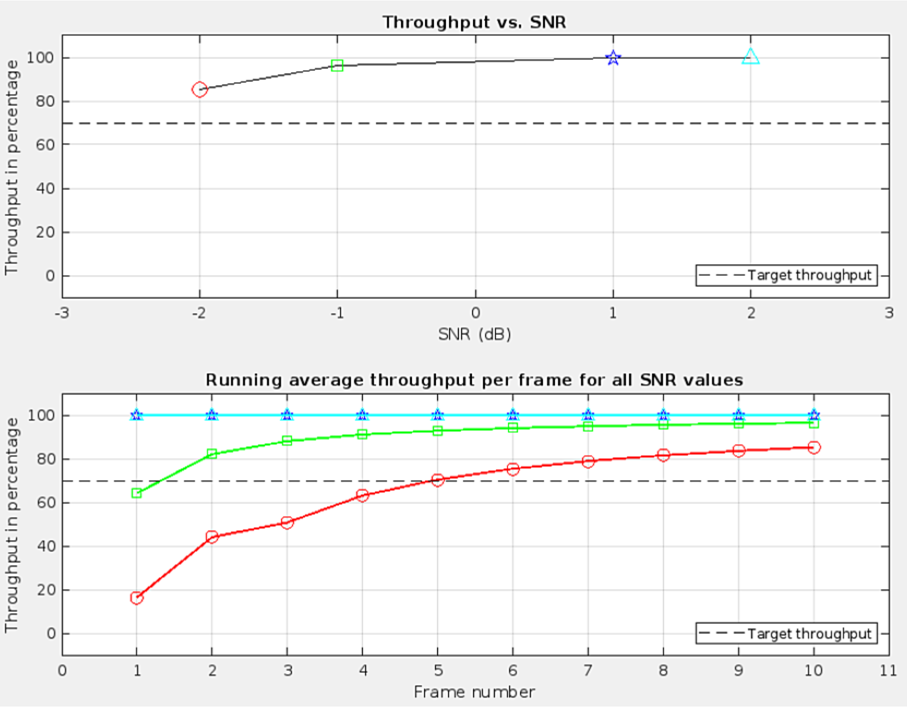

Fig. 4. Radio channel throughput and signal-to-noise ratio for channel 10 in the situation of transmission between components of an M2M system in an ideal radio channel

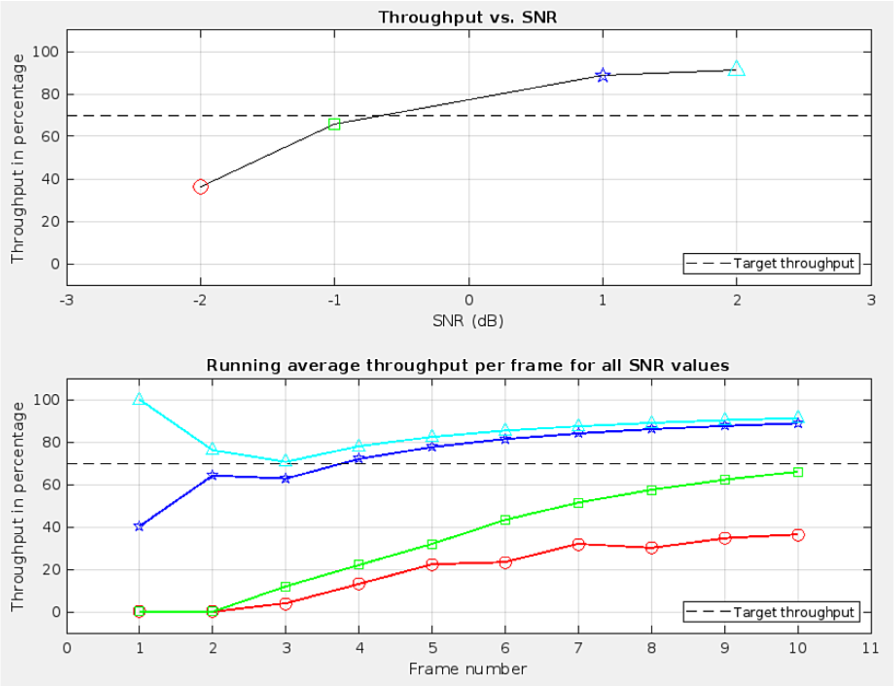

Fig. 5. Radio channel throughput and signal-to-noise ratio for channel 10 in the situation of transmission between components of an M2M system in a noisy radio channel

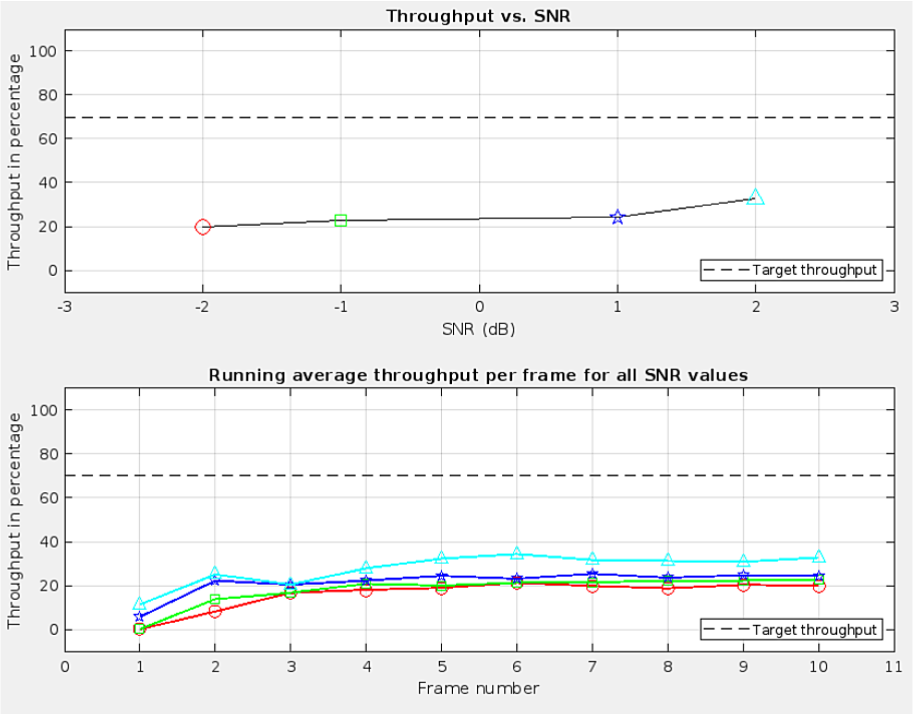

Fig. 6. Radio channel throughput and signal-to-noise ratio for channel 12 in the situation of transmission between components of an M2M system in an ideal radio channel

should be made for a correct process of building a mathematical model:

- The real object is assumed to be linear, with constant parameters, rigid solids; this leads to the dynamics of the object by means of linear differential equations of the order of two;
- Disturbances are assumed to have the property of being stationary in the wider sense and global ergodicity;
- Generalised coordinate systems have been adopted so that the trajectory of the solution can be compared with the trajectories

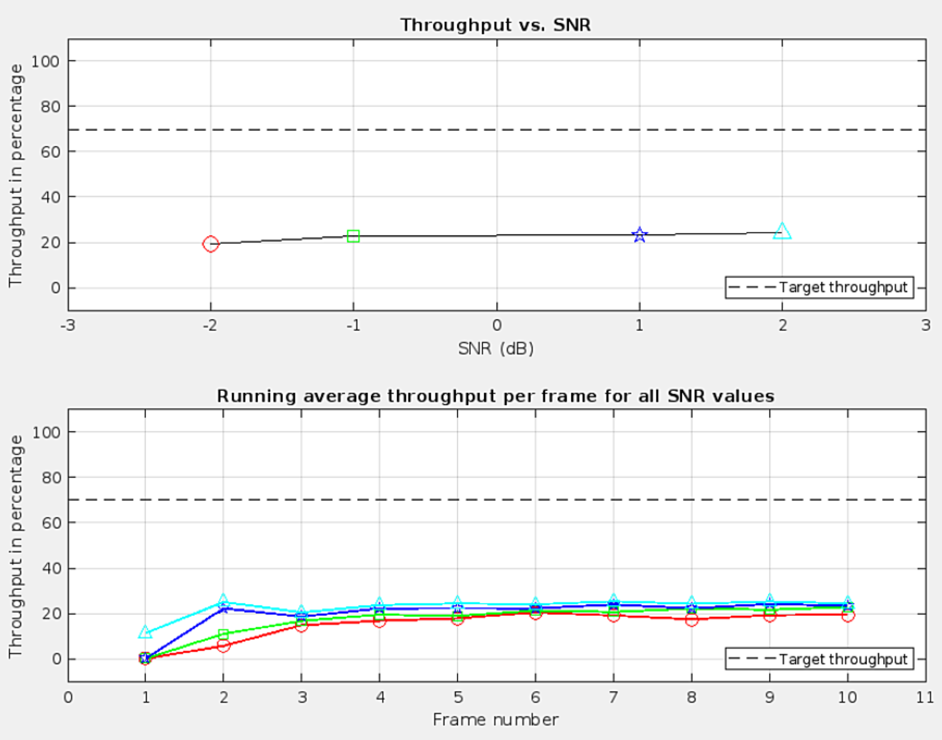

Fig. 7. Radio channel throughput and signal-to-noise ratio for channel 12 in the situation of transmission between components of an M2M system in a noisy radio channel

of movement of individual masses for the real object.

According to the assumptions as above, we can record the equations of mass movement of an object. The methods of formulating these equations are relatively complicated and for the purpose of this work we will not quote them, but only write down the names of the two basic ones that are used most often. Thus, the first method is Lagrange's equations, and the second is d'Alembert's equation. These can be found in the work Kisilowski [12].

The general form of linear equations is recorded in matrix form:

$$A\ddot{q}(t) + B\dot{q}(t) + Cq(t) = F(t), \qquad (1)$$

where: A, B, C – are matrices containing constants (mass-inertia, damping, elasticity);
q – is a generalised coordinate vector;
$F(t)$ – is a vector of extortion.

The properties of such a system depend exclusively on the parameters of matrixes A, B and C. Therefore, we can determine which parameters have an impact on the characteristics of the object whose changes may cause a threat. Thus, it becomes possible to define the relation between the parameters and the features that may pose a threat. For our course of action it is necessary to define the scope of change of parameters which should be kept in order to avoid a threat of a dangerous event. Defining the values of correct parameters will result in the creation of a barrier limiting the occurrence of threats in the risks under consideration. If the range of parameters is within the predicted range, the dangerous event will not occur. Thus, it is necessary to determine the relationship between the parameters and the selected characteristics (which may be the cause of a dangerous event).

From the elementary transformations you can get the equation:

$$\dot{x} = Gx, \qquad (2)$$

where:

$$G = \begin{bmatrix} -A^{-1}B & -A^{-1}C \\ I & 0_1 \end{bmatrix}, \quad x = \begin{bmatrix} \dot{q} \\ q \end{bmatrix},$$

$$dim\ A = dim\ B = dim\ C = dim\ I = \\ = dim\ 0_1 = n \times n,\ dim\ G = 2n \times 2n$$

I – is a unit matrix; 0_1 – the zero matrix.

This equation is called the state equation and the G matrix is the state matrix. For a state equation, the corresponding values and own vectors, which also apply to the mathematical model, can be determined (numerically), equation (1) [12]. The calculation can be performed for parameters of the real object. Eigenvalues are taken as an example of a selected feature of the system:

$$\lambda_j = a_j + ib_j \tag{3}$$

where: a_j – attenuation coefficient, if all a_j <, the fluctuations are attenuated, i.e. the movement of the object is asymptotically stable in the sense of Lapunov;
b_j – requency of oscillation with a period of $T_i = 2\pi/b_j$.

After transformations and numerical calculations, which can be found in the work by Kisilowski [12], the result is a dependency that allows to define an algorithm for calculations:

$$\frac{\partial \lambda_i}{\partial p_j} = \bar{k}_i \frac{\partial G}{\partial p_j} \bar{w}_i \tag{4}$$

where: $\bar{k}_i, \bar{w}_i$ – *i*-th vector and custom row.

So, after a full analysis, we found the dependence of the parameter imbalances on selected features of the system. The solution to this task may lead to an answer to the question which parameter may cause a disturbance of a characteristic influencing the creation of a threat. It should be added that the features of the object are selected so that they can be determined in the model and compared with the features of the real object. Most often these are signals coming from real objects, which can be directed to networks that manage the risk.

Technical diagnostic methods for determining the risk of danger

The second area that can be used to identify hazards leading to a quantitative risk assessment is the issue of using technical diagnostic methods to identify the risk of a hazard arising in any technical system. Let us quote here an approach that uses machine life curves to assess the condition of a machine. This task was discussed in detail in the works of Kisilowski et al. [10] and Kisilowski [13]. The condition of the machine is determined by means of symptoms. Symptoms of the machine can be e.g. vibroacoustic. More details on this subject can be found in the works of Cempel [3] and Morel [17].

Based on this work, a tribowibroacoustic model of the machine can be defined and described analytically (for a given symptom):

$$\frac{S(\Theta)}{S_0} = \left[1 - \frac{\Theta}{\Theta_b}\right]^{\frac{1}{\gamma}} ; \quad \Theta \subset \Theta_b \tag{5}$$

where: S_0 – initial symptom value;
$\frac{\Theta}{\Theta_b}$ – dimensionless machine wear time;
$\frac{1}{\gamma}$ – the machine wear curve exponent, determined according to the curve from Figure 8;
$S(\Theta)$ – symptom after time Θ;
parameters γ, Θ_b, S_0 – assessed on the basis of an experiment.

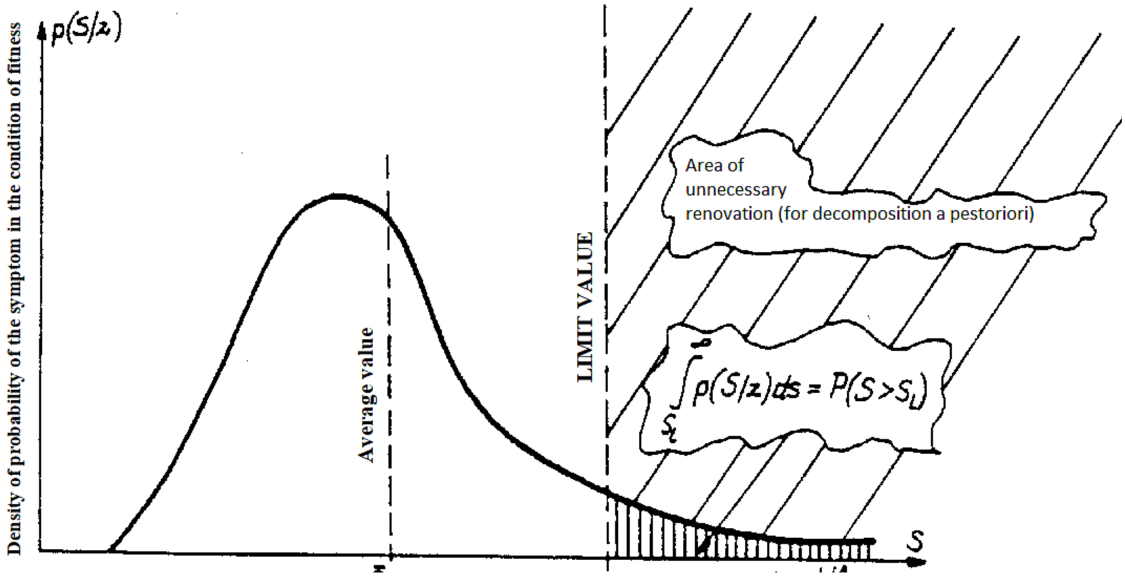

Fig. 8. Illustration of the baseline of a diagnostic probabilistic model to determine the *S1* limit value using Neyman-Pearson's statistical decision making theory [3]

The key problem in the implementation of the risk analysis process is the issue of assessing potential threats, including the hypothetical process of damage. Applying this approach means in practice carrying out a systematic analysis of the system's operation in order to detect and determine threats, including those unpredictable in normal operation and possible operational problems resulting from the existence of uncertainty as to the manner and intensity of degradation and wear processes.

With specific assumptions for load S and load L as random variables, a relationship can be made to the probability of failure as defined:

$$P_f = \int_{\Omega} f_{x_1 \ldots x_n} S(X_1 \ldots X_n) dX_1 \ldots dX_n \qquad (6)$$

Since the probability density function is most often unknown and the integration procedures in the equation (6) are cumbersome, appropriately simplified calculation techniques should be developed to calculate the probability of damage (failure), as shown in Kisilowski's work [13].

The procedure presented makes it possible to determine the probability of failure as a function of the service life of the machine. These parameters should be known in the network in which the equipment under assessment operates, e.g. LSN.

CONCLUSIONS

The studies presented show that it is worthwhile to use logistical social networks (LSNs) in crisis management, where modern techniques can be used, such as the Internet of Things (IoT) or Machine to Machine (M2M), which enable the collection of any amount of data in an LSN operating throughout the country, and even more widely. A computer simulation was also performed for sample data imaging the M2M system. The results obtained in the simulation show the feasibility of using the M2M system for preparing information for the LSN. The algorithm provides opportunities to extend the way information is created and generated. This is its primary advantage. The presented algorithm is a new IT element and cannot be compared to algorithms that do not currently exist in this field and have not been used in crisis management. Two quantitative methods are also presented for risk assessment and a procedure for communicating these results to the LSN, which is a tool in public crisis management. The methods presented allow them to be used in further work that will assess the potential for risk in various types of equipment and technical systems that may cause a crisis risk. In order to ensure public security in today's world, with such a broad taxonomy of threats, it is necessary to use mathematical and technical methods in crisis management to manage risks more effectively. Scientific research on security must be interdisciplinary in nature, taking into account all aspects of crisis management. However, it cannot be overlooked that the generation of more and more data makes the use of mathematical and technical methods also a necessity to ensure information security and define the limits of personal freedom. This does not change the fact that risks must be managed rationally and can be based on the mathematical and technical methods presented.

REFERENCES

1. Ahmad F., Marwat SNK, Zaki Y., Mehmood Y. and Görg C.: Machine-to-Machine sensor data multiplexing using LTE-advanced relay node for logistics. In: Kotzab H., Panek J., Thoben K.D. (Eds): Dynamics in Logistics, Proceedings of the 4th International Conference LDIC, Bremen, Germany 2014, 247-258.
2. Atzori L., Iera A. and Morabito G.: SloT: giving a social structure to the internet of things. IEEE Communications Letters, 15(11), Nov. 2011, 1193-1195.
3. Cempel Cz.: Vibroacoustic diagnostics of machines. PWN, Warsaw 1989.
4. Chang Y.-C.: Study of overload control problem for intelligent LTE M2M communication system. Advances in Smart Systems Research, 3(3), 2013, 44–48.
5. Directive 96/82/EC on the control of major-accident hazards involving dangerous substances called Seveso II Directive as amended by Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC, Official Journal of the EU L 197.
6. Haller S., Karnouskos S., Schroth C.: The internet of things in an enterprise context. In: The first Future Internet Symposium (FIS), Vienna, Austria, September 2008, 14-28.
7. INET Framework, Accessed: 21-July-2018, https://inet.omnetpp.org.
8. Kaplan S., Garrick B.J.: On the quantitative definition of risk. Risk Analysis, 1, 1981,11-27.

9. Kaplan S.: The words of risk analysis. Risk Analysis, 17, 1997, 407-417.
10. Kisilowski J., Kisilowski M., Radkowski S.: Technical diagnosis in risk assessment in property insurance. Diagnostyka 2000, II International Congress of Technical Diagnostics, Warsaw, Poland, 19-22 September 2000.
11. Kisilowski J.: An analysis of the parametric sensitivity of the eigenvalues of the linear mathematical model of a mechanical system. Building Machines Archives, 31, 1984, 3-4.
12. Kisilowski J.: Dynamics of the Mechanical System Rail Vehicle-Track. PWN, Warsaw 1992.
13. Kisilowski M.: Principles of insurance risk management for machinery and technical equipment, dissertation, Orgmasz, Warsaw 2002.
14. Kovac D., Masek P., Hosek J.: Simulation-Based Study on Capacity Performance of 4G Mobile Network for M2M Services, in the International Conference “Technical Universities: Integration with European and World Systems of Education”, Izhevsk, Russia, April 2014.
15. Masek P., Hosek J., Dubrava M.: Influence of M2M communication on LTE networks. In: The 10th International IEEE Conference, Zvule, Czech Republic, August 2014.
16. Mehmood Y., Pötsch T., Marwat SNK, Ahmad F., Görg C. and Rashid I.: Impact of machine-to-machine traffic on LTE data traffic performance. In: Kotzab H., Panek J., Thoben K.D. (Eds.): Dynamics in Logistics, Proceedings of the 4th International Conference LDIC, Bremen, Germany 2014, 259-270.
17. Morela J.: Vibration of machines and diagnostics of their technical condition. Polish Society of Technical Diagnostics, Warsaw 1992.
18. OREDA (2009), OREDA Reliability Data, OREDA Participants. Available from: Det Norske Veritas, NO 1322 Høvik, Norway, 4th Ed.
19. Rausand M.: Risk assessment, Theory, Methods, and Applications. John Wiley & Sons, Inc., 2011.
20. Setlak L., Kowalik R., Lusiak T.: Practical use of composite materials used in military aircraft, Materiale 2021, 14(17), https://www.mdpi.com/1996-1944/14/17/4812.
21. SimuLTE Modeler Version (0.9.1). Accessed: 21-July-2018, http://www.simulte.com