RISK VALUE MODELING IN DISTRIBUTED PRODUCTION ENVIRONMENT – IN AN ASPECT OF INFORMATION FLOWS' ANALYSIS

Jacek Woźniak

Wojskowa Akademia Techniczna

Abstract. In the article, author describes a subject associated with the analysis of the risk value in a distributed production environment. Main extent of reflections focuses on information flows, as a specific source of risk factors (threats) for the information (and not only) safety of the production company, operating in a distributed environment (networking). There are primarily the following issues discussed: identification of hazards in a distributed structure (taking the strategy of vertical and horizontal integration into an account). This characterizes the specificity of information flows and mechanisms of the knowledge management in a networking environment, assumptions of risk modeling (including Monte Carlo simulation), and the meaning of operational and historical data resources in knowledge creation processes (about the level of risk), described. The article is concluded by a presentation of four models of risk management in a distributed environment, based on three variables: the probability of an existence of a threat (P), the value of potential losses (L), and the number of risk factors (RF) in the ambient of a distributed production system. Presented models show changes in the value of risk (R) – as derivatives of changes of values of these parameters. Thus, they constitute the analytical and decision-making database for activities undertaken by managers at all levels of management.

1. Introduction

The article focuses on modeling a risk value in a distributed production environment. The primary area of this study is an information flows' phenomenon (between processes' participants) – with a partial connection to assumptions of the *information benchmarking strategy*. Information flows – taking a development of ICT[1] infrastructure, processes of globalization resulting in creation of production networks, e.g. in a transregional-, transnational- or global scale into an account – takes a particular importance in identification risk factors' sources. The article is dominated by the *pessimistic approach* to risk analyzing. However, there are also presented basic *positive aspects* of making a risk analysis in an area of information flows in a distributed environment.

There are presented relationships between the use of a potential of an analytical data processing and risk estimation in an article. Of course, forecasting a risk value is an essence of planning organization's activities. However, it should be aware that risk is an unstable and changeable phenomenon, determined by multiple – usually not

[1] Internet and Communication Technology.

correlated each other – factors. Therefore, *a risk value cannot be estimated precisely on a base of historical data*. There are lots of methods and techniques in a business practice which allow to estimate a risk value (closely to a real level), e.g. statistical methods. In order to present proper risk analysis' assumptions in a distributed production environment, there are presented *four general analytical model*s – which enable an observation of fundamental assumptions of a risk analysis in an article, taking two basic parameters: the value of potential losses and the probability of an existence of a threat into account.

2. Chosen assumptions of risk analysis in distributed production system

2.1. Organizational structure's integration strategy as a base of risk analysis

Management in conditions of distributed environment is determined by processes of both a **vertical**[2] and a **horizontal integration**[3]. However, it should be noted that in terms of risk analysis more important is a horizontal integration, understood as a combination (e.g. on a base of alliances[4] and strategic acquisitions) of various business units, e.g. suppliers and subcontractors. That phenomenon also directly reflects a specificity of network/distributed structures (fig. 1).

Taking assumptions of a risk analysis in a network environment into an account, it should be aware that a horizontal integration may increase a number of identifiable and active risk factors, mainly in terms of cost. This happens, because joining new units to the original structure results in generating additional costs – in the case of production system those can be fixed costs and overheads. This is a derivative of a phenomenon which shows that a horizontal integration is focused e.g. on exploration new branches or entering new markets (in order to broad a spectrum of an action). In this connection, additional costs may be: **cost of lost opportunities** (e.g. entry into another market than elected by the staff management) and **financial costs** (financing a horizontal integration[5]). However, specified above categories of costs should be seen both as a **derivative of information flows** in a distributed envi-

[2] A vertical integration should be understood as a technological combination of production, distribution, sales or other business processes [19].

[3] A horizontal integration takes form of sourcing or realizing an integration. This is a kind of an integration in which a company absorbs its own provider [20].

[4] More (in terms of an information management in a networking environment) (in:) [12, p. 243 et seq.].

[5] Financial costs include e.g.: interest on loans and advances, interest on arrears in payment, exchange losses, paid bills, bank fees, discounts, loss on disposal of investments and investment value update.

ronment and as a **source of errors and malfunctions in communication system's functioning**.

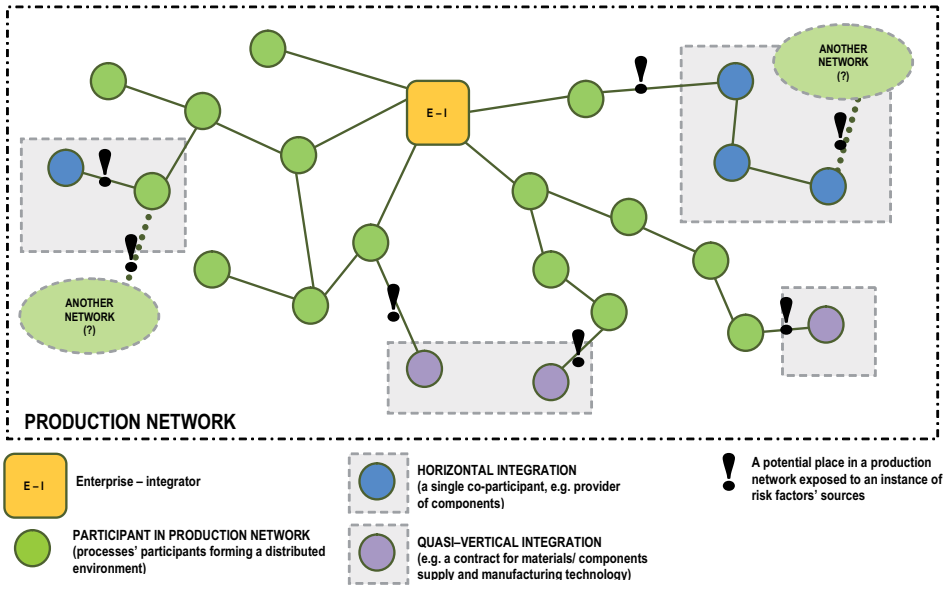

Fig. 1. Identification of risk factors' sources in a horizontal integration strategy. Source: own work

It should be noted that manifestations of a horizontal integration can also be identified in a vertical integration. A vertical integration in an organization may be proceed on four levels (also in an aspect of information flows' integration in a distributed environment). Selling and buying from independent business units, signing contracts binding two enterprises by a long-term contract, is called a **quasi-vertical integration**, that is a *relationship between enterprises* (what may be manifested e.g. through an acquisition of a majority of shares or joining research activities). The fourth level of vertical integration is called a **total vertical integration** and is understood as an incorporation suppliers or customers into an overall structure of the company. Therefore, it should be noted that an organization's integration – both vertical and horizontal – in terms of cost (and risk) analysis is more beneficial to larger enterprises, which may afford a higher cost level [19].

Of course, strictly cost factors are a direct base for analysis of an effectiveness and an efficiency of production processes. However, variations in these parameters in an indirect way initiate mechanisms of risk management. Having regard to the fact (which can even be considered as an axiom of economic research) that a purpose of any business unit is to maximize a value (mainly by maximizing a profit) – managing

a sphere of production costs[6] has become a fundamental element of risk management processes (both operational and strategic).

2.2. Specificity of risk analysis of information flows in distributed environment

Distributed environment – in an aspect of a network structure – is characterized by relatively large diversification of internal operators/units. Network of relationships is a derivative of an evolution of a widely understood business conditions.

Making analysis of a relationship between factors directly determining a state of a production system, it should be noted that a base of risk analysis' mechanisms are production factors' flows. This kind of situation takes on particular importance in the case of network structures[7]. Identification of risk sources in a distributed environment is realized in different, specific conditions[8]. This is due to the fact that analyzed relationships (initially *autonomously* functioning in a network) get a *holistic* nature, linking various processes' participants. In addition, created in this way an information and decisions determines functioning of *system models*.

In order to define an impact of network-natured production system on an efficiency of risk analysis processes, it must be specified the **Implement-organizing Risk Analysis Model in Network Production System** (1) firstly, which takes a following form:

$$IRM_{nps} = f(M_{c+r}, C_{is}, DP_{co}, P_f, KMS, O_{s+o}), \tag{1}$$

where:

IRM_{nps} – Implement-organizing Risk Analysis Model in Network Production System;

M_{c+r} – complexity of a network, relationships with external units (customers)[9], a degree of dispersion of an organizational structure;

C_{is} – internal system conditions/determinants;

DP_{co} – developing potential of participants in a network (co-participants) – e.g. in terms of information resources and specificities of analytical actions undertaken by a managerial staff and "lower levels" of workers;

P_f – production factors;

[6] Production is considered as one of three basic processes (along with a supply and a distribution) [3].

[7] See e.g. [in:] [8, p. 111 et seq.].

[8] Main levels and categories of a risk are presented [in:] [16, p. 20-29; 34-40], [10, p. 216-224].

[9] See also [in:] [14. p. 33 et seq.].

KMS – peculiarity of knowledge management system (taking an IT environment into an account – generally in terms of data obtaining by operational systems (OLTP[10]) and data processing in analytical systems (OLAP[11]) and a content of data repositories;

O_{s+o} – peculiarity of strategic objectives (a degree of concentration on targeted risk management) and operational objectives (e.g. identification and elimination of risk factors in *ad hoc* mode).

Therefore, the **risk degree** should be considered as a probability and a potential/capacity of a network to handle needs of market participants in this case (e.g. customers and suppliers) in order to achieve a system and market advantage [9][12], as well as a network's capacity for self-development, including improvement of internal relationships – mainly as a consequence of the **tacit knowledge diffusion**[13] between participants of a distributed organizational structure (processes' participants).

2.3. Conceptualy-analytical model of risk management in distributed environment

Generating a knowledge about a risk value using dependencies based on information flows in a distributed environment is an integral element of risk management. In pursuing a proper implementation and consuming decision-making capacity in a distributed environment (network) – with a focus on an efficiency and quality management (and terminally a value of a production system), it must be defined the **Conceptualy-Analytical Model of Risk Management** (2), which is a function of ten variables:

$$CAM_{rm} = f(MT_{rm}, C_{rm}, S_{rm}, C_{rf}, K_{ca}, AS_{f}, IE_{int}, RE_{met}, AV, E_{ra}), \tag{2}$$

where:

CAM_{rm} – Conceptualy-Analytical Model of Risk Management;

MT_{rm} – methods and techniques of a risk management (adapted to needs and requirements of individual relationships between co-participants in a network);

C_{rm} – a risk management cycle within an organization (a network structure);

[10] On-Line Transaction Processing.

[11] On-Line Analytical Processing.

[12] A value in a distributed production system should be seen in a similar way – see [in:] [8, p. 111--112; 139]. It should also be noted that a system value and a market position of an organization is a derivative of a risk analysis.

[13] A tacit knowledge diffusion in a network environment is described more widely [in:] [8, p. 116], [11, p. 106 et seq.].

S_{rm} – developed standards for risk management in a network structure (mainly between an enterprise-integrator[14] and other (rotating) participants of production processes);

C_{rf} – accumulation of quantity and value of risk factors between processes' participants and an enterprise-integrator;

K_{ca} – a status of current and actual knowledge in a network (about a risk level, as well as a potential and existing risk factors);

AS_f – a functionality and usefulness of an analytical systems in a distributed structure (mentioning both an IT systems, mechanisms and tools of a tacit knowledge management);

IE_{int} – a level of integration of an information environment in a distributed structure;

RE_{met} – methodology of estimating a risk value[15], either for a distributed structure (in a system analysis), as well as for individual information flows;

AV – an added value chain in a production network – which allows to quantify sources of individual risk factors and thereby improve a quality of conducted system risks analysis (both in a strategic and *ad hoc* approach);

E_{ra} – an efficiency of carried out risk analysis (both in an elementary and a holistic approach)[16].

It should be noted that presented model (2) takes multiple dimensions of risk management determinants in a production system into an account. Indeed, this model shows a necessity to use in analyses not only distributed data sources, but also directly organizational-natured factors – primarily in terms of implementation of new methods and techniques of management and creation generally-networking standards for risk analysis, widely understood (e.g. through the prism of human resources – i.e. a tacit knowledge and an increase in a system value) analytical potential of applied concepts of management. This is a **flexible model**, taking the variability and dynamics of a network (a distributed production system) into an account. Thus, there is also a possibility of that model's adaptation during an implementation of concepts and methods of a knowledge diffusion in a network environment[17], which, as mentioned in this chapter, is a base of a properly conducted iterative cycle of risk management.

[14] An *enterprise-integrator* plays a primary role in a production network and is responsible for a state of a final product – and thereby both a general/system and elementary risk analysis. See also [in:] Chapter 2.4.

[15] Methods of estimation risk value (in an aspect of project management) are presented [in:] [10, p. 224-246].

[16] More (in an aspect of an added value creation by individual system's elements) [in:] [16, p. 76-77].

[17] See [in:] [11, p. 51 et seq.].

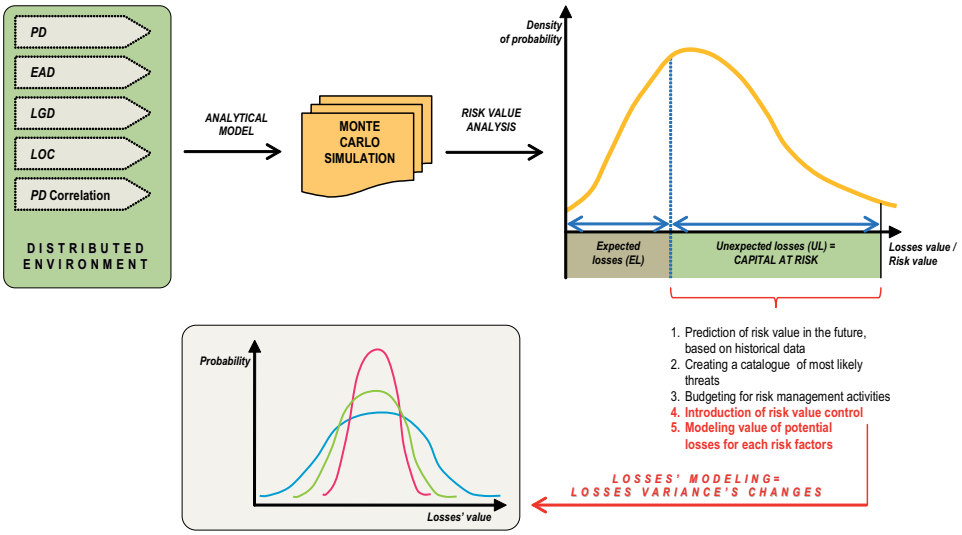

Fig. 2. Process of Monte Carlo simulation – in an aspect of risk factors' diversification and losses' modeling. Source: own work based on [6]

In order to analyze threats with a use of the Conceptualy-Analytical Model of Risk Management (2), it should be aware a phenomenon of identification and estimation a value of a **total capital at risk**. In theory, one of the most popular methods is a *Monte Carlo simulation*[18] (fig. 2). It enables a characterization of different risk categories – taking **specific risk parameters** into an account [6] (tab. 1).

Monte Carlo simulation enables estimation of a value of **total losses (*TL*)** (3), which are a sum of sets: **expected losses (*EL*)** and **unexpected losses (*UL*)** [6]:

$$TL = EL \cup UL. \tag{3}$$

Moreover, unexpected losses can be treated as a **capital at risk**, i.e. a sum of inputs (in a form of an owners' equity) necessary for maintaining or restoring the continuity of a network operation at the moment of threats' occurrence [6] (here: in an area of information flows which determine e.g. production-logistic processes). Capital at risk (unexpected losses) should be understood as a set of all possible to occur kinds of risk (4):

$$UL = CR = RS = \{R_M, R_B, R_O, \dots\}, \tag{4}$$

[18] Within the Monte Carlo simulation a project model (of information flows) is calculated repeatedly (iterate). Input values are selected randomly for each variable for each iteration – based on a probability distribution for that variable. This is the way of calculating a probability distribution for total costs [1, p. 314].

where:

CR – a capital at risk;

RS – a set of risk sorts' value – important from the point of system management (production network) in a distributed environment;

R_M – a market risk;

R_B – a business risk;

R_O – an operational risk.

Making analysis of dependencies (3) and (4), it can be concluded that a value of losses related to an existence of a risk in an area of information system (in a production network) is a sum of both costs (inputs) of the current safeguard of a continuity of a system's (production processes') operations, as well as certain costs (and other threats) at a level of relationships between co-participants in a network – *mostly in terms of a horizontal information integration* (fig. 1).

It should also be noted that a Monte Carlo simulation refers to assumptions of statistical analysis, using a probability distributions for a risk value[19] (fig. 2). There has to be a necessity to identify a value of a variance of potential losses – allowing to manipulate their level (in a form of controlling of a risk level) in order to estimate a probability of specific threats' existence at a base of this type analysis – what is intended to determine the most precise value of a capital at risk [6]. These type forecasts assume particular importance in a case of a distributed manufacturing network's operations. Due to the multiplicity and complexity of relationships between processes' participants, simulation in generally-system approach may be difficult (or even impossible) to carry out. Recommended action should rather be making simulation with the use of Monte Carlo model assumptions on "the lowest level of network's detailing" – that is for individual business relations. Thanks to this approach, there is a possibility to proper management of risk categories – listed in table 1 – in a case of analyzed phenomenon.

At this point, it should be shown the methodology of estimating an elemental risk in a production system. For the purpose of this study, it is assumed that a risk analysis (related to information flows) should be based on a presence of particular kinds of threats. This happens because each, even the least important economic event, is correlated to specific risk factors [5], [7], [16]. In order to its proper identification, company's executives should first and foremost analyze following cost determinants

[19] Continuous probability distributions show a level of an uncertainty connected e.g. with costs [1] of information flows' realization in a distributed environment – what justifies a possibility of estimating a capital at risk (*CR*). Continuous distributions have shapes corresponding to typical data obtained during a risk analysis. Examples are: triangular distribution, Beta distribution and normal distribution [1, p. 312].

of risk: **level of potential losses**[20] **(*L*)** [5], **probability of an existence of a threat**[21] **(*P*)** [5], as well as **quantity of risk factors (*RF*)** in an organization's ambient (and more precisely – in an aspect of production process). All specified above risk factors determine a **value of a risk**[22] **(*R*)** [5].

Tab. 1

Risk parameters in Monte Carlo simulation methodology and most likely risk categories

Risk parameters	Definition	Most likely risk categories[1] in an area of information flows in distributed production system
Annual rate (AR)	Frequency or intensity of risk per year	1. Management and responsibility 2. Costs' structure 3. Procedures and control tools 4. Choice of subcontractors 5. Product and service offer
Probability of Default (PD)	Probability of risk occurrence	1. Costs' structure 2. Marketing and market share 3. Knowledge and trainings
Exposure At Default (EAD)	Maximum value of losses in terms of an occurrence of risky event	1. Production interruptions and breakdowns 2. Loss of operational continuity[2] 3. Inputs and investment strategy
Level Of Control (LOC)	Level of risk control	1. Costs' structure 2. Poor quality of products and services 3. Product and service offer 4. Inputs and investment strategy 5. Production interruptions and breakdowns
PD Correlation	For various types of risk	---
Loss Given default (LGD)	Statistical level of losses after risk realization	---

Source: own work based on [6]

[1] On a base of research conducted by PhD Z. Krysiak in 2010 year. See [in:] [6, p. 39].

[2] An issue of a business continuity of a process organization's operating in conditions of losing an information continuity is described more widely [in:] [15].

[20] As an equivalent of a value of an *EAD* parameter.

[21] As an equivalent of a value of a *PD* parameter.

[22] As an equivalent of a value of an *UL* parameter.

2.4. Processes of knowledge diffusion

A knowledge diffusion plays a crucial role in a risk analysis in a network structure. This is due to the complexity and specificity of internal relationships. Indeed, it should be remembered that a network of relationships between various processes' participants is characterized by the lack of internal competition. There is no typical form of "market competition" – specific to a market economy (e.g. for a monopolistic economy model). Therefore, flows of production factors determine a condition of autonomous (of course, in some sense) risk factors' existence. There are identified production risks as a derivative of an disability to implement a specific task by participants in a production network. At this point, however, it should be considered whether this situation can arise in current economic realities (?). The answer is as follows – network is a flexible structure, which selects co-participants according to their capacities.

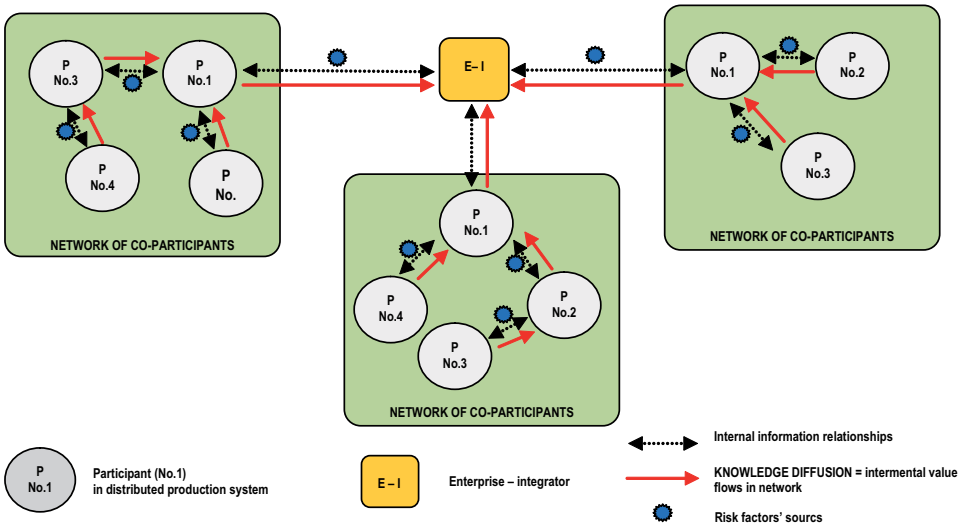

Fig. 3. A knowledge diffusion – in terms of a risk analysis in a distributed production environment
Source: own work

Therefore, what may be risk sources in an information-natured network? Having regard to processes of digitalization increasing in the world of business, as well as permanent processes of globalization, there can be indicated following sources of risk factors associated with production factors flows in that situation:

– a specificity of information flows between different processes' participants – associated mainly with the bandwidth of communication chan-

nels, e.g. regarding an availability of materials, semi-finished products, human resources and technology;
- incorrectly realized processes (or their lack) of transactional data repositories' sourcing and/or analytical data processing;
- a lack of ICT infrastructure accordingly expanded in an enterprise – this is a problem frequently noted in the sector of SMES, from which micro-, small- and medium-sized enterprises are usually basic and technologically specialized links in a production networks;
- an absence or disability to carry out an integration of information environments (distributed databases) between enterprises shaping a current production network.

Presented above potential sources of risk factors are associated with an occurrence of the **information benchmarking**[23] phenomenon.

Moreover, a tacit knowledge diffusion mentioned above, plays a key role in processes of identifying, monitoring and a risk analysis, as well as preventing results of risk appearance and/or reducing their effects. A knowledge passed between specific/individual links of a production chain (in a network) is undergoing processes of consolidation and verification, generating knowledge resource in a system terminally – reflecting a specifity of a network and thus having a high level of an added value in terms of a risk analysis (fig. 3). A knowledge possessed by an each participant regards to typically specified activities (an element of a production chain). Thus, a tacit knowledge (which undergoing e.g. processes of externalization, socialization and combination)[24], deriving from a selected and single production link, has a chance to become a base of risk analysis not only in an area of current co-participant's operation, but also can be used for necessities of an entire network (or their parts). This kind situation has an essential meaning generally in the case of identification a potential of risk factors and taking preventive actions, e.g. by an enterprise-integrator.

[23] The essence of an *information benchmarking* is associated with basic assumptions of the *benchmarking conception*. Benchmarking is a specific kind of a comparison one organization (business unit) to another (which is called as a *benchmark*) – a comparison to: internal structures is an *internal benchmarking*, organizations from the same industry is an *external benchmarking* and an organizations from different industries is a *functional benchmarking* [4], [18]. An information benchmarking can be understood as: learning from the best benchmark by comparing them (e.g. in connection with an optimization of information processes), seeking the most efficient methods for information resources management, permanent evaluation of such activities in the light of competitors' achievements, specific kind of innovative process and a process of continuous improvement of activities in an information aspect. Replication of other business units can take two forms: replication of external organizations, not related each other by business processes or imitate an external benchmark incorporated to a process structure – there should be noted relations with (referred in this article) strategies of a horizontal and vertical integration in this case.

[24] According to assumptions of the *Knowledge Spiral Conception* created by I. Nonaka and H. Takeuschi.

3. Principles of functioning and a place of information flows strategy in process-configured organization

3.1. The importance of operational information system for information flows

Information flows, as previously noted, can take two forms: learning how to manage information resources, as well as obtaining certain data categories. Therefore, it can be concluded that it is largely associated with functioning of the *operational information system*. On the one hand, information flows are responsible for data obtaining – which are important from the point of view of a production system. On the other hand, it can be a source of improvements in functioning of an operational information system as an integral entire. For example, returning to parameters of an efficiency and quality, it should be noted that information flows are capable to source following categories of information patterns/standards of operation (which are collection of information resources simultaneously obtained from other co-participants in a network):

1) the way of functioning of an information system, its strengths and weaknesses;
2) main, current sources of threats to a process of information flows strategy implementation;
3) an impact of taken decisions in the *ad hoc* mode on changes of an efficiency and quality value (of production processes in an information environment of benchmarks);
4) main categories of information needs to be taken into an account in analysis of an efficiency and quality;
5) an impact of current analysis of parameters on a state of a production system and its resistance to the presence of identified threats;
6) a compilation of necessary methods, techniques and tools to carry out a comprehensive measurement of parameters of production processes;
7) a relation between efficiency and quality of production processes (the strength of the correlation).

In addition, those patterns of action should not be seen solely through the prism of sourcing distributed operational data. They affect an efficiency of an operational information system functioning, as well as the whole organization, e.g. as a result of:

- satisfying current information needs of a production system [2];
- supporting short-term decisions, mainly in cost and time dimensions;
- carrying out complete and multiaspected control, e.g. of an efficiency and quality in an *ad hoc* mode;
- sourcing analytical data repositories [17];

– providing specific and required information resources to process teams – functioning within the framework of a production system, especially teams responsible for costs (in terms of efficiency) and individual components of quality (both finished goods and added value)[25].

In conclusion, it should be noted that information flows have a huge impact on the way of functioning of an operational information system. Moreover, it allows not only to create a favorable environment for obtaining action patterns in terms of transactional data management, but also absorbing specific categories of information about production processes (and not only[26]) from benchmarks.

3.2. Analytical data resources and implementation of information flows strategy

An analytical information system of a process-configured organization enables primarily implementation of such actions of process teams, like [17]:

– a multidimensional analysis of historical events in a production area;
– evolution of parameters/dimensions of those analyses – mainly in order to obtain detailed and concrete output (data)[27], necessary during decision-making processes;
– generating reports, e.g. regarding an efficiency and quality of production processes, as well as their constituent factors (reliability, completeness, usefulness, costs, time);
– creation of a complete information environment to implement actions based on data exploration – e.g. in terms of analyzing relations between an efficiency of production and its quality and an impact of that correlation on individual production subprocesses and a condition of a production system (often also of a whole organization).

Therefore, it can be concluded that an analytical information system is used mainly for long-term improvement of a company – a production system in this case. However, there should be considered a role played by information flows in this situation. Moreover, it shall be responsible for an ongoing obtaining of certain categories of data and best practices from co-participants. It is also important that a collection of transactional data developed in this way, can become a base for an analytical information system [17] (fig. 4). This is an indirect dependency. It should

[25] Example sources of information flows' categories in terms of other business units (as a possible competitors) analyzing are presented [in:] [9, p. 44].

[26] According to assumptions of system's perception, it should be remembered that a production process is directly determined by other processes, e.g. HR, financial, logistics – that also determine a value of an efficiency and quality of a production system.

[27] A process of data obtaining from an ambient is presented [in:] [9, p. 45].

therefore be considered whether there is a form of direct relationship between an analytical information system and information flows[28]. Having regard to the fact that an organization is able to derive from other business units (e.g. benchmarks[29]) different action patterns – specific to operational activities – it may be seen that there is also a chance to get information about long-term and proved action patterns.

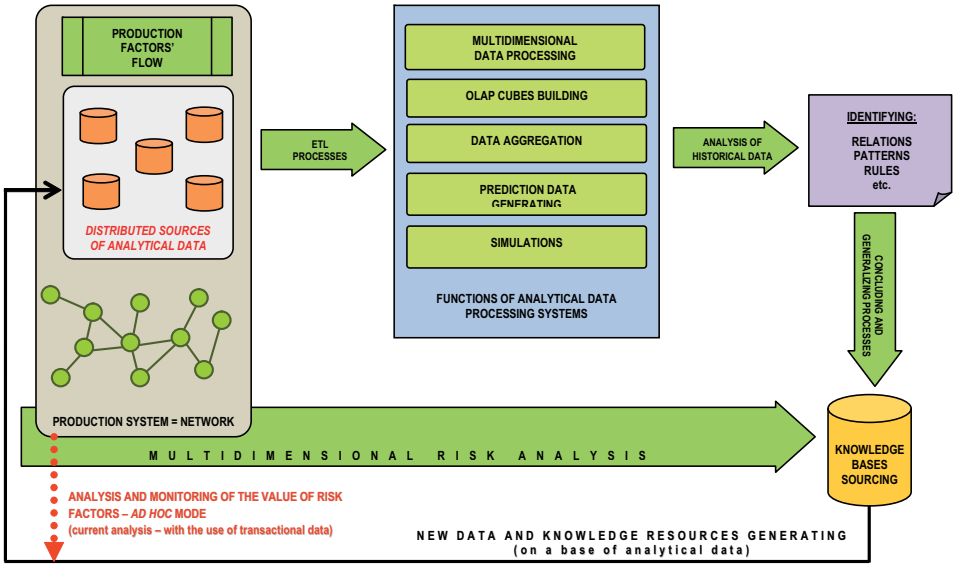

Fig. 4. Application of analytical systems' (OLAP) functions in a risk analysis and a knowledge generating processes in a distributed production environment. Source: own work

However, it should be remembered that these patterns may be unsuitable and impossible to adapt in an environment of production system. So far, in terms of transactional activities differences between individual organizations can be eliminated (e.g. in *ad hoc* mode), unfortunately, there is no analogical solution (or possibility) in terms of analytical information systems. Implemented pattern, e.g. in a case of an analysis of an efficiency with the use of its specific determinants (not reflecting specificity of current organization), results in the receipt of the report "falsifying" (despite an accuracy and truthfulness of results) a decision-making area. Actions based on this type of patterns can be seen as an additional generator of costs (which also reduces an efficiency of a production system).

[28] Analytical information systems use in information flows focused on creating market advantage are presented [in:] [9, p. 131-138].
[29] See [in:] Chapter 2.4.

Having regard to analysis of implementation's conditions of an information flow strategy in an analytical data environment, it must be noted a necessity of respecting basic safety requirements. As known, an information flows strategy bases on maintaining permanent contacts with external units/participants. In addition, sharing resources and action patterns, a co-participant (e.g. a benchmark) also can expect such an information support (and usually does so)[30]. It also shows that there cannot be taken a long-term cooperation in an aspect of information flows – just because of benchmark's requirements in terms of getting a feedback, unfortunately, highly sensitive for an organization (an obtaining one).

This type situation takes on particular importance in terms of a production system. Organizations operates in the experience economy[31] and the widespread phenomenon of products substitution. Companies try to prepare its offer for individual customers and satisfy their autonomous needs [9], [14]. Providing a benchmark "key" categories of data on the principle of "reciprocity" may results in a long-time in weakness of a market position of an organization. Thus, an information flows strategy will not generate expected results, becoming a source of business-natured threats and additional costs. At this point, it should also be made a reference to an analysis of costs and risk presented in previous chapters. It should therefore be noted that information flows in analyzed area of an enterprise's performance are not recommended for a broad, multifaceted implementation. Relations based on data exchange should rather concern "less sensitive" areas – from the viewpoint of autonomy, as well as the continuity of processes/production systems[32].

However, if there is a "risky" relation (described above) in a production system, it should also be noted a necessity to implement solutions based on the *information asymmetry* (both in a transactional and analytical information system) [13]. This type actions allow to precise define *end users* of data categories shared with co-participants (e.g. benchmarks). Of course, an information asymmetry does not reduce significantly a risk level e.g. of data disclosure to unauthorized users (units, participants). However, it may limit undesirable effects in some sense.

In conclusion, it can be noted that information flows play an important role in the way of operating of an analytical information system. It can be a source both of obtaining historical data and specific action patterns. It also may be associated with

[30] Therefore, in the case of an internal and functional benchmarking, threats associated with disclosure of valuable resources and simultaneous weakening of an organization is relatively small (because a benchmark from an another industry does not threatens directly the market position of an enterprise and may become a long-term business co-worker – what in a situation of raising in an efficiency – of its specific information areas – will be able to support production processes), but there is a high level of a risk in a case of an external benchmarking.

[31] According e.g. to an added value.

[32] See more [in:] [15].

variable risk categories, which are able to significantly violate an information stability (and not only) of an enterprise in a long term. Therefore, an information flow strategy should be implemented judiciously, taking care of an aspect of data (held and shared) safety and a quality of obtained resources and action patterns.

4. Modeling of a risk analysis

There is presented an analysis of three separate models related to an implementation of an information flows strategy in an enterprise's information system and its impact on a risk value both in a short and long term in this article. However, it must be clarified basic assumptions for all three models at the beginning:

1) risk value (R) is a product of losses (L) and probability of an existence of a threat (P)[33] (5) [5]:

$$R = L \text{ x } P. \tag{5}$$

So that, it can be noted – according to relations (4) – that capital at risk (CR) is a product of exposure at default (EAD) and probability of default (PD) (6):

$$CR = EAD \text{ x } PD. \tag{6}$$

2) number of risk factors (RF) in an ambient of an organization is constant for a short and a long period of time;
3) value of losses (L) and probability of an existence of a threat *(P)* are variables in time and may show an ascending or descending trend.

There is a necessity to indicate additional assumptions – which are contained in table 2, in order to make an analysis of **specified three risk models**.

There should be considered the form of main determinants in **MODEL 1** (fig. 5) at this moment. Major sources of such way evolution of values of an each parameter should be found in incorrect security policy. An increase in value of losses (L) is a large result of a strong relationship between obtained action patterns and data sources and an effectiveness of production processes, and even their activities' continuity. The importance of information resources which are

[33] There can also be taken other factors, such as: *the exposure factor* which characterizes a level of a process' exposure on a threat, *susceptibility* which determines a degree of process' exposure on risk, as well as the *number of risk repeats* – an expected number of risk instances during a process's realization into an account (in this analysis of a risk value). However, for clarity reasons of an analysis, those factors had been omitted, focusing an attention on two fundamental determinants of a risk value: a probability of an existence of a threat and a level of losses.

a derivative of an information flows strategy and a level of losses exhibit a simple dependency – the higher rank of information resources is granted, the higher expected level of losses as a result of improper functioning of an information flows strategy in an organizational environment is observed. Decrease in the probability (*P*) can be a result of correct tad expected operation of the security system for each category of information resources. There is played an important role by the audit of a quality of obtained action patterns and information from co-participants in this case.

Tab. 2

Specified risk models and basic differences between their assumptions

Model	**Chosen parameters**					
	Level of losses (L)		***Probability of an existence of a threat (P)***		***Risk value (R)***	
MODEL 1	Continues to grow during a length of time of an information flows strategy implementation.	↑	Decreases during an increase in the period of information flows.	↓	Is getting lower in a short period of time, while in long period of time is getting higher. *optimum* The point with the lowest value of risk is *the optimum*, designated in a place of intersection of *P* and *L* curves.	↓ ↑
MODEL 2	Continues to grow with a length of time of an information flows strategy implementation.	↑	Grows with an increase in a period of information flows.	↑	Continues to grow during a length of time of an information flows strategy implementation.	↑
MODEL 3	Decreases during an increase in a length of time of an information flows strategy implementation.	↓	Decreases with an increase in a period of information flows.	↓	Decreases during an increase in a length of time of an information flows strategy implementation.	↓

Source: own work

In conclusion, it should be noted that MODEL 1 reflects a negative aspect of an implementation of an information flows strategy in a process organization. That is mainly due to the fact that a level of losses is increasing systematically. Despite the fall in a value of probability of an existence of a specific risk factor (threat), in a long term currently analyzed strategy determines a dramatic increase in a risk value. Obviously, it should be noted that a certain threat category does not have to happen in a practice – parameter *P* is at low level. However, if that threat occurs, it will cause large losses.

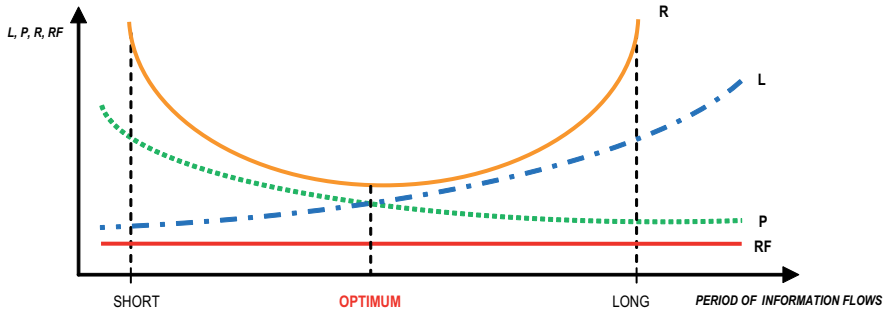

Fig. 5. A risk value and its main determinants – depending on a length of an information flows relationship – MODEL 1. Source: own work

For **MODEL 2** (fig. 6) a main source of an increase in a value of a parameter *L* – similarly as in the case of MODEL 1 – should be considered in terms of a strong relationship between obtained action patterns and data sources and an effectiveness of production processes in an enterprise. In turn, an increase in a probability (*P*) may be a result of malfunction of a security system of each category of resources and the lack of an information audit – as a result, there are approved untested or unadjusted patterns in an organization (this is a result of an incorrectly made benchmarks' selection). Moreover, obtained data – according to assumptions of that model – may be incorrect (out-of-date, false, defective, etc).

Thus, MODEL 2 can be considered as a reflection of the most unfavorable situation for a company and its information system (in terms of an information flows implementation). A risk value increases permanently – relatively slow in a short period, but rapidly in a long one. Taking an assumption of a long-term cooperation between different organizations into an account, executives should take remedial action in the case of activities associated with both a parameter *P* and parameter *S*. In this way, it can be possible to move to another model – MODEL 1 (more favorable, but not enough stable and safe for an information environment in an organization) or MODEL 3 (most favorable for an organization which implement an information flows strategy).

There is (like in two previous models) assumed an existence of a strong correlation between a value of information resources and an effectiveness of production processes in **MODEL 3** (fig. 7). However, observed decrease of a level of losses (*L*) in a long term may e.g. be a derivative of a low-value assets (information) in this class (eg. analytical or operational), a dispersal of data sources or a tight security system (e.g. ICT tools). Moreover, a decrease of probability of an existence of a threat during an implementation of an information flows strategy may also derive from a proper functioning of a security system of each category of information resources and permanent monitoring of changes in an organization (e.g. in terms of changes' forecasting in an area of specific risk factors).

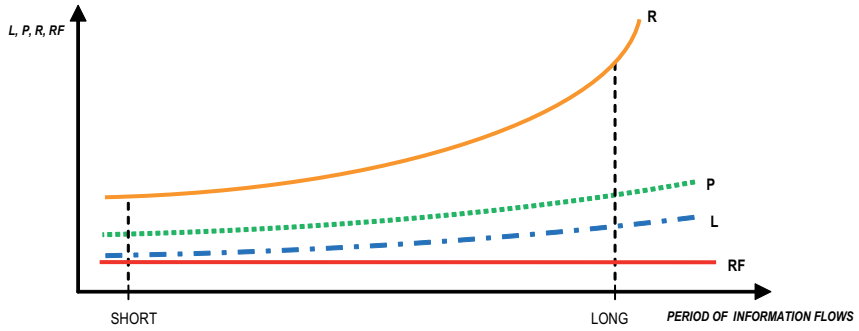

Fig. 6. risk value and its main determinants – depending on a length of an information flows relationship – MODEL 2. Source: own work

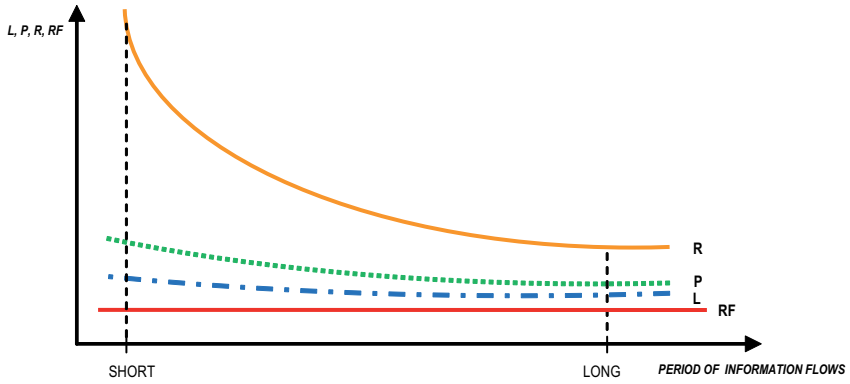

Fig. 7. A risk value and its main determinants – depending on a length of an information flows relationship – MODEL 3. Source: own work

Therefore, it should be noted that despite a high risk value (*R*) in a short period of an information strategy implementation (what may be associated with an increase in a level of costs adjusting an information system to other co-participants standards – fig. 1), over time, is systematically reduced, given relatively low and stable value in the long-term. This type of situation requires from executives (mainly) special attention at a stage of planning and implementation actions of the strategy. In a situation of eliminating major threats (or proper eliminating their negative effects on information flows' processes), there is an opportunity for organizations to achieve a success in a long term.

There should also be seen the legitimacy of **MODEL 4** implementation – characterized by a decrease of a value of parameter *S*, and an increases of a value of parameter *P* in an article. However, taking assumptions which are similar to those, that had been given in MODEL 1 into an account, MODEL 4 will not be characterized separately.

3. Implications for a management area

In order to make a conclusion of presented analysis, dependencies and models in article – associated with modeling of a risk value in terms of information flows in a distributed (networking) environment, it should be aware quantification of following conclusions:

1) Risk management is an iterative, continuous and complex process. It requires both a holistic (system) approach, a s well as an elementary one. Therefore, a risk management should be carried out at all levels of a process management. Only such an approach could bring expected results.
2) A distributed production environment is characterized by different determinants of a risk analysis. This situation is determined e.g. by: a change in a nature of external business units (a competitor becomes a co-participant in a networking relationship), a modification of communication channels – basis on flattening of relationships, as well as an approach to the identification of risk sources in a network.
3) Important elements in risk modeling are processes of knowledge management – what is usually skipped by executives and managers at other organizational levels. A knowledge about a system is a useful source of information regarding, e.g. changes in a relationship with co-participants (which may be a source of identification of new threats!), or changes in an ambient. Moreover, a knowledge management in a distributed environment is a complex phenomenon, requiring a holistic approach and precision from managers.
4) A proper risk management (especially in an area of modeling risk dependencies) should base on historical data resources. An ability to analyze the past generate

a large potential to explore the future. However, it cannot be forgotten that risk is also a complex and hardly predictable phenomenon. Thus, the reliance solely on an analysis of historical data may not be sufficient — and worse, it may be a source of additional risk factors. Therefore, an important role is played by a knowledge and an experience of the decision-maker in this case.

5) Modeling of changes in an area of risk may be a base of analytical operations and decision-making in a distributed production system.
6) Modeling a risk value, which is a derivative of its evaluation, complements a risk management process, which is predominantly connected with a stage of forecasting and planning activities.
7) A risk value depends on several variables. The choice of these important factors, which should become a base of a risk analysis (as well as modeling of changes of its value over time) depends on specifics of an organization and a current situation. Not always are important the same variables. An example might be here a *Monte Carlo simulation* which takes 5 variables into an account – while four risk models (presented in an article) are based only on 3 variables.
8) Making an analysis of risk according to an implementation of an information benchmarking strategy in an environment of process organization, it cannot be explicitly specified an estimated risk value. The way of an evolution of certain cost determinants is correlated to specific circumstances of an information environment. What more, a risk value, according to analyzed above models, is only a decision-making information (e.g. in the context of planning preventive actions in accordance with *ex ante* model). It does not need to have a major influence on an actual state of processes e.g. determined by an information benchmarking.

To sum up, a risk management is a necessary phenomenon in current business conditions. However, this is a complex and multifaceted area. Thus, this article is aimed exclusively on selected aspects of a risk management – with a particular focus on risk value modeling in distributed production environment (in terms of an information flows' analysis).

REFERENCES:

1. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Fourth Edition. Wydanie polskie*, Project Management Institute, Warszawa 2009.
2. B. Bińczycki, M. Tyrańska, J. Walas-Trębacz, *System informacyjny w zarządzaniu operacyjnym* (Information system in operational management), AE, Kraków 2007.
3. A. Bitkowska, *Zarządzanie procesami biznesowymi w przedsiębiorstwie* (Process management in enterprises), VIZJA PRESS & IT, Warszawa 2009.
4. J. Brilman, *Nowoczesne koncepcje i metody zarządzania* (Modern conceptions and methods of management), PWE, Warszawa 2002.

5. E. Gancarz, S. Zając, *Zarządzanie ryzykiem* (Risk management), „Nowoczesne Systemy Zarządzania, Zeszyt nr 2" („Modern Management Systems, Vol. 2"), WAT, Warszawa 2007.
6. Z. Krysiak, *Wartość ryzyka* (Risk value), „Kwartalnik Nauk o Przedsiębiorstwie, nr 2/2011(19)" („Enterprise Science Quaterly", no. 2/2011(19)", SGH, Warszawa 2011.
7. M. Łada, A. Kozarkiewicz, *Zarządzanie wartością projektów* (Value management of projects), C.H. Beck, Warszawa 2010.
8. S. Łobejko, *Przedsiębiorstwo sieciowe. Zmiany uwarunkowań i strategii w XXI wieku* (Network enterprise. Changes in circumstances and strategies in the 21st century), SGH, Warszawa 2010.
9. Z. Malara, J. Rzęchowski, *Zarządzanie informacją na rynku globalnym. Teoria i praktyka* (Information management in the global market. Theory and practice), C.H. Beck, Warszawa 2011.
10. A. Manikowski, *Ilościowe metody wspomagania ocen projektów gospodarczych* (Quantitative methods to support evaluation of economic projects), Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa 2010.
11. K. Perechuda, *Dyfuzja wiedzy w przedsiębiorstwie sieciowym. Wizualizacja i kompozycja* (Knowledge diffusion in a networking company. Visualization and composition), AE, Wrocław 2007.
12. C. Shapiro, H.R. Varian, *Potęga informacji. Strategiczny przewodnik po gospodarce sieciowej* (Information Rules: A Strategic Guide to the Network Economy), Harvard Business School Press, Helion, Gliwice 2007.
13. J. Woźniak, P. Zaskórski, *Asymetria informacyjna w zarządzaniu bezpieczeństwem organizacji procesowych* (Information assymetry in security management of process organization), „Nowoczesne Systemy Zarządzania, Zeszyt Nr 4" („Modern Management Systems, vol. 4"), WAT, Warszawa 2009.
14. *Wybrane aspekty marketingu relacji (*Selected aspects of relationship marketing), (ed.) A.K. Krzepicka, WAT, Warszawa 2007.
15. *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania* (Organization management in conditions of risk of losing information continuity of operating), (ed.) P. Zaskórski, WAT, Warszawa 2011.
16. *Zarządzanie ryzykiem działalności organizacji* (Risk management of organization activities), (ed.) J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa 2010.
17. P. Zaskórski, *Strategie informacyjne w zarządzaniu organizacjami gospodarczymi* (Information strategies in business organizations management), WAT, Warszawa 2005.
18. K. Zimniewicz, *Współczesne koncepcje i metody zarządzania* (Contemporary conceptions and methods of management), PWE, Warszawa 2009.
19. http://rsastrategicsolutions.com/strategia-integracji-pionowej.php, z dn. 14.07.2011.
20. http://www.wiedzabiznesu.com.pl/artykul/integracja_horyzontalna_pozioma, z dn. 11.07.2011.

Modelowanie wartości ryzyka w środowisku rozproszenia produkcyjnego – w aspekcie analizy przepływu informacji

Streszczenie. W artykule prezentowana jest tematyka związana z analizą wartości ryzyka w rozproszonym środowisku produkcyjnym. Głównym obszarem rozważań są przepływy informacyjne jako specyficzne źródło czynników ryzyka (zagrożeń) dla bezpieczeństwa informacyjnego (i nie tylko) przedsiębiorstwa produkcyjnego, funkcjonującego w środowisku rozproszonym (sieciowym). W artykule poruszone są przede wszystkim kwestie związane z: identyfikacją zagrożeń w strukturze rozproszonej (z uwzględnieniem strategii integracji pionowej i poziomej), charakterystyką specyfiki przepływów informacyjnych i mechanizmów zarządzania wiedzą w środowisku sieciowym, założeniami modelowania ryzyka (z uwzględnieniem symulacji Monte Carlo), a także w znaczeniu zasobów danych operacyjnych i historycznych w generowaniu wiedzy na temat poziomu ryzyka. Artykuł zakończony jest prezentacją czterech modeli zarządzania ryzykiem w środowisku rozproszonym, bazujących na trzech zmiennych: prawdopodobieństwie zaistnienia ryzyka (P), wartości potencjalnych strat (L) oraz liczbie czynników ryzyka (RF) w otoczeniu rozproszonego systemu produkcyjnego. Zaprezentowane modele obrazują zmiany wartości ryzyka (R) przy określonych zmianach wartości wspomnianych parametrów. Stanowią zatem bazę analityczno-decyzyjną dla działań podejmowanych przez menedżerów na wszystkich szczeblach zarządzania.