ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 105

1st International Scientific and Practical Conference on Digital Economy (ISCDE 2019)

On the issue of risk structuring of the use of Internet of things technologies in logistics

Kaftannikov I.L.
South Ural State University
Chelyabinsk, Russia
kaftannikovil@susu.ru

Dzenzeliuk N.S.
South Ural State University
Chelyabinsk, Russia
dzenzeliukns@susu.ru

Zhernov A.P.
IP Zhernov A.P.
Chelyabinsk, Russia
Logitek74@mail.ru

***Abstract* — Internet of Things technologies are being implemented in all spheres of human activity. The application of such technologies and elements of cyberphysical systems is especially active in areas equipped with a large number of various devices and systems. Logistics is one of these areas. From the one hand, using the Internet of things technology and elements of cyber-physical systems allows to reduce the risks of the so-called human factor, but, from the other hand, information risks arise and amplify associated with the processing of information circulating in the logistics turnover. The article provides a classification of various types of risks that may arise during the operation of the Internet of things technologies. The main classification criterion is the use of information at various stages of the logistics chain, which is one of the main entities in logistics. The article also provides recommendations on minimizing possible risks.**

Keywords — internet of things in logistics; cyberphysical systems in logistics, risks in logistics.

I. INTRODUCTION

Logistics is a field of activity that provides for the distribution of goods in a wide range, from local deliveries to global delivery of goods around the world. At the same time, along with an increase in the number of delivered goods, the variety of possible ways to ensure supplies increases.

Along with this, supply chains suffer a significant transformation. Supply chain is one of the main logistic elements due to new technologies [1]. Logistics companies commonly used means of identifying products in all parts of the supply chain using Internet of things technology new opportunities. This allows for global distribution optimization, and thereby reduce the downtime of equipment, deliver goods at the right time and place, etc. At the same time, with the absolute positive effects of the information use, and more precisely, digital technologies, a number of new risks arise that can undermine the company's reputation, as well as lead to a decrease in profits. The article provides a structural analysis of these risks.

Modern Internet of things technologies provide great opportunities for the formation, transformation, monitoring, analysis, decision support and other information services, which is required in today's global, customer-oriented markets. At the same time, the receipt, processing and analysis of data for all stages of the supply chain, in most cases, is carried out without the direct involvement of a person. From the one hand, it minimizes the risk of so-called "Human factor", from the other hand, global information access leads to the emergence of new risks that did not take place during the traditional organization of supplies.

II. RESEARCH METHODOLOGY

The Internet of things technology and elements of cyber-physical systems using allows, from the one hand, to reduce the risks of the so-called human factor, but, from the other hand, information risks arise and intensify. Such risks are associated with the depersonalization of objects of information processes throughout the sequence of the supply chain. Along with the problems of depersonalization, the problems of leakage of personal data become relevant.

In the era of digitalization, the responsibility boundaries of subjects of logistic relations are changing; and if in the process of implementing traditional logistics it can be argued that each cycle and its internal business processes are under the control of a responsible person or group of people, then with the introduction of Internet of things technologies, the redistribution of responsibility boundaries takes place, and it becomes more difficult to determine whose competence is to a different business process, since control is carried out by cyber-physical entities.

Risks arise as a result of possible imperfections, failures of algorithms, i.e. have the technological nature of digital processing. It is impossible to deny a possible deliberate external impact on the information environment, providing decision-making in the supply chain.

In order to conduct a qualitative analysis of possible risks using the Internet of things technologies and elements of cyberphysical systems in the field of logistics, it is necessary to have an idea of the main essence of logistics - the supply chain. The supply chain (network) is a multi-valued concept and is defined differently in different sources. For example, as a combination of all types of business processes (design, production, sales, service, procurement, distribution, resource management, supporting functions) necessary to meet the demand for a product or service - from the initial moment of

receipt of raw materials or information to delivery of goods or providing services to the end user [2].

In another case, the supply chain is defined as follows: supply chain is a coordinated system composed of manufacturers, retailers, and consumer markets. In this system, under the guarantee of the interests of all aspects, they cooperate with each other and influence each other [3]. (The supply chain is a coordinated system consisting of manufacturers, retailers and consumer markets. In this system, under the guarantee of the interests of all parties, the component systems cooperate with each other and influence each other.)

Obviously, the models which include the information based on the presented definitions will be different.

Since there is a focus on a set of risks arising in the Internet of things, it should be mainly analyzed the risks associated with information processes accompanying or determining those. In this case, these are the risks of information transformation during the implementation of production processes (for example, data on the parameters of raw materials and components at the input to the production, determined by the automatic input control system, in which not only errors of the first or second kind may occur, but also other distortions or lack of information), information errors of directly technological processes, as well as production transport errors that occur when moving material resources inside or between repartitions.

There are also risks of information distortions in the formation of the output data of the products. In aggregate information risks at the output of production can be represented as

$$Rp = Rin + Rtn + Rtr + Rout \quad (1)$$

where

Rp - information production risks;

Rin - input information risks;

Rtn - technological information risks;

Rtr - transport information risks;

Rout - risks of generating output accompanying information.

Traditionally, the composition of the supply chain is described as follows [4]:

- Purchasing cycle;
- Manufacturing support cycle;
- Market distribution cycle.

III. RESEARCH RESULTS

In order to formulate a system of possible risks when introducing Internet of things technologies and elements of cyber-physical systems, it is necessary to consider in detail each stage of the supply chain. When considering each stage, the business processes characteristic of this stage are highlighted and a pool of risks is formed that can arise during the implementation of a particular business process.

In purchasing cycle the output information supply risks are determined by the information support of the following business processes:

- procurement of materials;
- purchase of component parts;
- placement and storage of materials or raw materials;
- possibly the purchase of equipment for production.

At this stage, risks can be defined not only as input parametric risks, but also as risks of inconsistent specifications of orders and inbound deliveries.

Raw material resources should be provided with input control parameters, which requires the use of appropriate equipment. In many ways such control will be carried out without human intervention, which leads to the emergence of new risk types.

So, for example, for the business process “procurement of materials” the following risks are characteristic:

- determination of the parameters of materials for their compliance with the requirements of production technology with non-certified equipment;
- verification by certified, but outdated equipment (not passed intermediate verification);
- failure of the equipment, or untimely warning of a malfunction;
- failure of the components of the information system responsible for the input control of material resources, etc.

The business process “procurement of components” is similar to the previous, in addition to the above risks, may include additional risks not peculiar to “procurement of materials”:

- identification of the purchase source, verification of the components parameters.

The business process in which the storage and / or placement of purchased materials, raw materials, elements and components takes place, despite its simplicity, is very important. The need for the proper organization of this business process is determined by the speed of response to changing market needs, and, consequently, the implementation of the order. As in the case of previous business processes, at this stage of the “Purchasing cycle” stage, there is the possibility of realizing the following risks:

- the storage of certain raw materials or components requires special climatic conditions. There is a risk of not maintaining the temperature regime, humidity for materials and raw materials.

Often, the biggest problems can bring the purchase of equipment to continue operations. The risks here may be as follows:

- lack of compatibility of newly delivered parts of equipment with the existing one;
- mismatch of specifications or other information support equipment.

To minimize such risks, it is necessary to develop appropriate procedures and expand the functionality of equipment for the implementation of self-monitoring, since in the era of digital transformations it is not a person (specially trained) who measures the parameters, keeps records where at the output from these processes there should be values of suitability for production, which leads to the risks of information disruptions.

It is possible to minimize these risks by taking the following steps:

a) Digital marking of input materials or places of their storage (sites, warehouses, other premises);

b) Development of control procedures for testing equipment;

c) Carrying out procedures and conditions for verifying the consistency of specifications determined by orders and deliveries.

Like the previous one, the production cycle contains many technological processes and the corresponding information transformations (for example, at the entrance of a rolling mill - a metal ingot, at the output - a sheet slope or profile or rail rolling, etc.) includes many business processes, such as:

- delivery of materials and components in accordance with the technological passports of production;
- timely delivery from internal warehousing places to production units;
- internal technological cycles of redistribution and assembly, in turn consisting of many subcycles;
- testing of manufactured components and devices based on or with the inclusion of these components;
- packaging and warehousing of finished products.

Information support of this stage is quite complicated, since it is here that information on sets of interrelated technological processes is generated, formed, converted and used, which ensures their coordination and production with the planned design parameters.

In addition, modern production should have model and modernization flexibility, as well as the ability to quickly update the range to meet consumer demand. Accordingly, within the framework of this stage with the indicated business processes, for example, the following risks may arise:

- lack or insufficient exact implementation of technological processes of production (which is often observed in illegal production schemes);
- lack or insufficiency of technological parameters control;
- insufficient quality of technological regulations or their support.

Low informational support of the production phase, noted in a number of some information systems, leads to risks of incorrect decision-making or to inconsistency of the parameters of the manufactured products with the parameters indicated in the accompanying documentation.

It should be noted that similar risks can arise during the internal transfer of components and materials, at the work in progress stage, as well as during testing and packaging of goods.

All processes of physical distribution cycles can be divided into “static” and “dynamic”. The former are based on pre-concluded transactions, confirmed by contracts, when most of the transaction parameters are known in advance, including the conditions of distribution. At the same time, even such “static” transactions do not guarantee successful cooperation and the exact fulfillment of contracts. Unforeseen risks, in the form of the appearance of reasons preventing the parties from fulfilling obligations under the contracts and arising due to the lack of preliminary information about them, are called force majeure. Such risks and the reaction of the parties to them are described by special articles of contracts. But even this can be ineffective.

By “dynamic” is understood deliveries carried out on the basis of a preliminary assessment of the supply parameters and forecasting the results of their implementation. Obviously, the main role here is played by forecasting tools, since how much the company can predict the position and quantity of the goods ordered determines the profit from the sale of goods. In addition, it is necessary to organize the competent storage of such goods, as well as an advertising company. One of the sad confirmations of this thesis is information on the value of discarded products in Russia in 2016, which amounted to approximately $ 24.6 billion [11].

The basic physical distribution cycle involves the following business processes:

- Integral customer order in a general form, determined using analysis and forecasting tools;
- Formation of the order;
- Processing and distribution of the order;
- Picking order;
- Transportation;
- Delivery to the final consumer.

These fundamental business processes can occur when there are threats of various types of risks. So, for example, the “Consumer Order” business process includes the following risks:

- incorrect reporting of the order / components;
- informational failure;
- leakage of personal data of the consumer (customer);
- unwanted expenses that can result in an automatic order or its incorrect configuration;
- data loss as a result of an open data transfer protocol and lack of data encryption;
- the risk of failure in the system for generating an order identifier.

When transferring a product or an order, there are primarily risks of an informational nature, namely:

- informational failure;

- errors in addressing the order, which can lead to economic losses.

The business process “Order Processing” is also in most cases subject to a type of risk with an informational character:

- informational failure of accounting systems;
- incorrect identification in various aspects: both the identification of the customer and the order directly;
- many of the existing solutions are proprietary, autonomous, unrelated to each other, which can lead to various types of inconsistencies and failures [5].

Order picking is a very crucial stage of the distribution cycle, at which risks such as:

- incorrect arrangement of elements will lead to incorrect assembly of the order;
- identification errors;
- failure of monitoring systems [5].
- at the time of order picking, an order identifier (initial identifier) is generated, data about which may be unreadable, may be displayed incorrectly in the system, a failure can lead to the fact that another product is present under this identifier;
- change in the area of responsibility, possibly changing identification parameters
- incorrect orientation of loaders and unloaders, risks of primary storage
- exit from the warehouse - change in the area of responsibility, transport system of the "last mile".

It is worth noting that the risks related, for example, to the concept of a “zone of responsibility” do not cause particular difficulties in the case of control of logistic processes by a person or a group of people, since the corresponding technologies and information support were created and debugged for decades. But the formal description of these processes to ensure control of business processes by automatic devices is very difficult. This is due to the possibilities of work and decision-making by a person in conditions of fuzzy or incomplete information and the insufficient level of capabilities of modern artificial intelligence to solve such problems.

There are types of risks when transporting goods, that are characteristic not only in the field of research, but rather traditional:

- failure to ensure the integrity of transit goods (lack of ability to control location, temperature, humidity and other indicators necessary for the delivery of goods intact);
- transport accidents due to incorrect indicators of self-driving machines or automatic controls (e.g. auto deceleration), as well as ordinary traffic accidents;
- accidents in the warehouse caused by incorrect settings of the work / sensors of the loaders (e.g. falling pallets);
- a consequence of the previous paragraph - injuries to employees [6];
- incorrect reading of sensors about temperature, humidity and as a result - incorrect storage;
- loading from one transport system to another can lead to a malfunction in the accounting system for orders and goods.

At the final stage of this stage - “Delivery to the consumer”, the following risks are also possible, which are largely characteristic of the previous stage:

- transport accidents due to incorrect indicators of self-driving machines or automatic controls (for example, automatic deceleration in case of danger).

It should be borne in mind that the exchange of information about the supply chain and its processing is not limited by the level of the business process, but also includes a huge amount of data, both from devices and sensors (elements of the Internet of things), and from applications for social networks and much more [7].

In addition to the indicated risk structure based on a technical malfunction or a human factor, it is impossible not to note the fact that the legislation, in particular in the Russian Federation, which regulates the sphere of logistics, often comes down to the Civil Code of the Russian Federation [8], legislation in the field of transportation [9] and international law [10]. In the era of digital transformation 4.0 much attention needs to be paid to protecting the information entered into the circulation of the logistics network. The lack of legal insecurity can also be attributed to the risks of logistics activities in general.

IV. CONCLUSIONS

The initial risk analysis of Industry 4.0 in the field of production and its logistics component shows that, with the transition to the Internet of things, the structure and composition of risks is changing. The main change is associated with the displacement of a person from the control, communication, analytical and other areas related to information support and business process support. On the one hand, this leads to a reduction in the risks associated with the so-called “human factor”. On the other hand, the algorithms for the operation of formal (digital) systems under conditions of complete certainty still lag behind the ability and ability of a person to determine the goals and objectives of an activity, to analyze and make decisions.

To date, the success of the intellectualization of cyberphysical objects and systems for working in conditions of insufficient and fuzzy information, poorly defined tasks still lags behind human capabilities, despite some successes in the field of recognition and machine learning. Accordingly, this leads not only to the risks of information support for production associated with the current and alleged participation of cyberphysical systems in all areas of production. These risks are associated with non-human forms and methods of information processing and decision making, as well as the resources and reliability of the cuberphysical systems. Which in turn requires the development of new approaches, methods, assessments, forecasting, reporting, responsibility, etc. in the environment of cyberphysical

systems. Some risks are presented in this paper, but it will take a lot of resources, time, research and hard work to represent, describe and structure the risks of Industry 4.0.

References

[1] Gawankar, Shradha A.; Gunasekaran, Angappa; Kamble, Sachin. A study on investments in the big data-driven supply chain, performance measures and organisational performance in Indian retail 4.0 context. INTERNATIONAL JOURNAL OF PRODUCTION RESEARCH, 2019.

[2] Grigor'yev, M. N. Kommercheskaya logistika: teoriya i praktika/ M. N. Grigor'yev, V. V. Tkach, S. A. Uvarov. — 3-ye izd., ispr. i dop. — Moskva : Izdatel'stvo Yurayt, 2019.

[3] A complementarity model and algorithm for supply chain with immediate marketing order Автор:: Pan, Guirong; Chen, Haodong; Sun, Hongchun JOURNAL OF MATHEMATICS AND COMPUTER SCIENCE-JMCS. Volume: 20 Issue: 1 Pages: 50-57

[4] Bowersox, Donald J. Supply chain logistics management Donald // J Bowersox, David J Closs, M. Bixby Cooper SUPPLY CHAIN LOGISTICS MANAGEMENT Published by McGraw-Hill Companies, Inc. 2002, p57

[5] INTERNET OF THINGS IN LOGISTICS. DHL Trend Research | Cisco Consulting Services. A collaborative report by DHL and Cisco on implications and use cases for the logistics industry. Availiable online: https://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf

[6] Amazon robot sets off bear repellant, putting 24 workers in hospital. Availiable online: https://www.theguardian.com/technology/2018/dec/06/24-us-amazon-workers-hospitalised-after-robot-sets-off-bear-repellent

[7] V.P.Kupriyanovskiy, S.A.Sinyagov, A. A.Klimov, A.V.Petrov, D.Ye. Namiot. Tsifrovyye tsepi postavok i tekhnologii na baze blokcheyn v sovmestnoy ekonomike. International Journal of Open Information Technologies ISSN: 2307-8162 vol. 5, no.8, 2017

[8] The civil code of the Russian Federation (part four): Federal law № 230-FZ of 18.12.2006. “Rossiiskaya gazeta”, 22.12.2006 (in Russian)

[9] “On Transport and Forwarding Activities”: Federal Law №. 87-FZ of 30.06.2003; “The Charter of Road Transport and Urban Ground Electric Transport”; Federal Law №. 259-FZ of 08.11. 2007

[10] Convention on Road Traffic, Vienna 11.08.1968; Convention on the Contract for the International Carriage of Goods by Road (CMR), Geneva 05.19.1956

[11] Podschitana stoimost' vybroshennykh rossiyanami produktov https://yandex.ru/news/story/Stoimost_vybroshennykh_rossiyanami_produktov_ocenili_v_16_trln_rublej--d1f01f07a7cdfaed2c7b5fa41592df87?%20lr=%20213&lang=ru&stid=OE65GNBuUVGhLdmeYidD&persistent_id=75914254&rubric=personal_feed&from=story