European Research Studies Journal
Volume XXIV, Special Issue 4, 2021

pp. 143-161

Creating Reliable and Resilient Logistics Organizations for Unpredictable Conditions and Unexpected Future

Submitted 16/09/21, 1st revision 01/10/21, 2nd revision 25/10/21, accepted 30/11/21

Lech A. Bukowski[1], Paweł Sobczak[2]

Abstract:

Purpose: *The objective of this paper is to develop a general concept for creating resilient logistics organizations under the deep uncertainty that arises from unpredictable conditions and unexpected future, and to integrate it with a framework for ensuring the reliable operation of these organizations under conditions of predictable change.*
Design/Methodology/Approach: *The research methodology was based on a transdisciplinary approach because logistics organizations have the nature of complex systems with different types of systems such as physical, cybernetic and social ones. The research approach used is based on a critical analysis of the literature and case studies from the authors' own experience. The research is supported by Ackoff's 'idealized design' approach and assumptions from The IRGC Risk Governance Framework.*
Findings: *It was found that complex logistics organizations can be successfully modelled as Engineered System of Systems and managed according to the principles applicable to such systems. Furthermore, it was shown that it is possible to combine two different concepts, namely High Reliability Organization and Resilient Enterprise, into one coherent whole in the form of a Reliable and Resilient Logistics Organization.*
Practical Implications: *For practical use of the developed concept, a framework was designed in the form of an algorithm describing the process of creating Reliable and Resilient Logistics Organization in the form of successive stages of action and decisions.*
Originality/value: *The concept of the Reliable and Resilient Logistics Organization is wholly original and is the result of many years of our research into the behavior of complex socio-technical systems under uncertainty. The added value of the work is the model developed, which in the form of a framework can be used in practice in logistics organizations to ensure their continuous and effective operation under various conditions, both predictable and unpredictable changes in the environment.*

Keywords: *Logistics organization, reliability, resilience, governance, deep uncertainty.*

JEL classification: *D21, D81, L22.*

Paper Type: *Research study.*

Acknowledgement: *"The project is funded under the program of the Minister of Science and Higher Education titled "Regional Initiative of Excellence" in 2019-2022, project number 018/RID/2018/19, the amount of funding PLN 10 788 423,16"*

[1]*Prof. of Management Engineering, WSB University in Dabrowa Górnicza, Poland, e-mail: lbukowski@wsb.edu.pl*
[2]*PhD., The same as in 1, e-mail: psobczak@wsb.edu.pl*

1. Introduction

Modern logistics networks are characterized by a topology of complex network structures that perform specific functions, consisting of moving in space and time, as well as storing goods in an efficient and effective manner, in a changing and uncertain environment with possible disturbances and threats. We understand logistics as a transdisciplinary field of knowledge regarding the effective and efficient implementation of flows (movement and storage) of tangible and intangible assets (goods, persons, transactions, and related information) within systems consisting of enterprises, their clients and other stakeholders (Bukowski, 2019).The key condition for the success of the main logistic activities – delivering products from the place of origin to the recipient – is a comprehensive approach to the entire system consisting of infrastructure and logistics processes, with particular emphasis on their complexity, imperfections of knowledge and broadly understood risk.

The challenges facing modern logistics networks result from the trends in the development of new technologies, especially information and communication technologies, as well as from the current state of the global economy, which is still in the phase of dynamic changes. Therefore, the improvement of competitiveness in the scope of logistic services requires continuous improvement of logistic processes, with particular emphasis on reliability, safety, and security aspects. The most important directions of activities improving the functioning of modern supply chains an networks can be described by (Pfohl, 2016):

- Increasing financial liquidity through active management of working capital, such as: inventories, receivables and financial liabilities;
- Refocusing of supply chains from the perspective of supply to the perspective of demand, through flexible and agile response to market needs (Demand Driven Supply Chain);
- Consolidation and at the same time regionalization of supply networks, allowing for a substantial reduction in transport costs and the number of warehouses;
- Improving the reliability, safety and security of the supply network by reducing their vulnerability to external threats and hazards related to both the forces of nature (e.g. natural disasters), as well as the intentional actions of criminal or terrorist groups;
- Increasing the resilience of the supply network to threats and hazards and the ability to maintain the supply continuity in crisis conditions;
- Strategic and comprehensive approach to risk management and governance in supply networks as a tool supporting key logistics decisions.

Therefore, the problems related to the vulnerability of logistic systems are among the most important challenges currently faced by people dealing professionally with logistics. However, this issue is presented in books only to a small extent, because most of the authors focus on issues related to the work of logistics systems only in

'normal' conditions (Blanchard, 2015; Gudehus and Kotzab, 2009; Harisson, van Hoek and Skipworth, 2014; Lasch, 2014; Nyhuis and Wiendal, 2009; Pfohl, 2016). The submitted work aims to partially fill this gap and build the basis for further exploration of this important issue.

The aim of this work is to synthesize current knowledge in the field of designing, testing and evaluation of logistic networks subjected to disturbances from a variable and uncertain environment, and on this background to present a new concept of reliable, safe, and secure product delivery assurance. The concept was based on the following four assumptions (Bukowski, 2019):

1. The complexity of logistics systems and the emergent nature of their properties. Modern supply chains are complex engineered system of systems (typically with a network structure) whose properties, due to multiple interdependency relations between their elements and the environment, are of emergent character.
2. A comprehensive approach to logistics systems requires consideration of three basic aspects, namely: the spatial extension of the logistics infrastructure and its environments, temporary continuity, and variability of logistics processes in life-cycle perspective and sustainability, and a holistic approach from a technical, economic, and socio-ethical perspective.
3. Imperfection of available knowledge and the expertise of decision-makers. In practice, knowledge is based on uncertain, incomplete, and ambiguous data and information, therefore it is imperfect. Furthermore, decision-makers are guided, especially under stress, by the principle of limited rationality which means a large impact of the subjective assessment of both the current situation and the outcome of the decision taken.
4. Modern logistics networks should be designed and implemented to provide them with the highest possible level of reliability, security, safety and resilience. Thus, one of the basic objectives of logistics management, both strategic and operational, should be rational risk and continuity management, with particular emphasis on disruption-tolerant operating.

The concept of the Reliable and Resilient Logistics Organization (RRLO) should be an adequate response to these problems. In developing it, the authors relied on a document established by the International Risk Governance Center called *The IRGC Risk Governance Framework* (IRGC, 2017). Based on these universal assumptions, the authors propose to assume that each complex logistics organization can be modelled as a System of Systems consisting of four core systems and one metasystem. The core of the system is a *meta-system*, whose role is to ensure continuous and uninterrupted communication between the individual systems through reliable information flow. This is followed by an analysis of the advantages and disadvantages of known management concepts for such organizations, namely High Reliability Organization (HRO) and an idea of Resilient Enterprise (RE). Based on this analysis and the authors' own experience, an RRLO concept was proposed that combines the advantages of both concepts and minimizes their weaknesses. In the final part of the

article, a framework for the application of the developed concept is presented in the form of an algorithm that can support the practical implementation of the RRLO concept.

2. Logistic Organization as an Engineered System of Systems

In recent decades, both engineered (man-made) and natural (social and ecological) systems have increasingly been considered comprehensively as large-scaled and highly sophisticated complex organizations. These systems have restrictions on information structure and critical sensitivity to risks. In reply to the emerging features and increased demands for control, the paradigm of *Large-Scale Systems (LSS)* has appeared in the system theory. A system is large-scale, if it has at least the following three main attributes: ability to decompose, centrality for geographical distribution and complexity (Keating, 2005).

System of Systems (SoS) is a natural extension of Large-Scale Systems (LSS). The concept of SoS represents a mix of independently operating and actively interacting large systems, integrated with sophisticated goals. The specific problems of SoS can be generalized in the following directions: determining appropriate list of independent LSSs for execution of task, assessing uncertain environment influence during SoS operation, and ensuring operative compatibility (interoperability) between SoS components (Jamshidi, 2005; DoD, 2008; Bukowski, 2016).

Engineered System of Systems (ESoS) is a set of heterogeneous subsystems assembled purposefully together to achieve a common goal that any system alone cannot fulfil, while maintaining the operational and managerial autonomy of each of the subsystems. These subsystems must be able to communicate and to work harmoniously together as well as to adapt their behavior and functioning locally when facing any change of their environment (Jamshidi, 2011), which in practice means concentrating activities on choosing and assembling these subsystems as well as designing appropriate interfaces to facilitate the reliable communication between individual parts of the system (Bilal *et al.*, 2014). Subsystems are selected and involved according to their potential roles, available resources, competences, and know-how that can be shared to fulfil the SoS objectives.

The process of creating ESoS from subsystems is called *architecting*. The purpose of the architecting process is to provide the required properties to the created systems. The most important required properties are (Billaud *et al.*, 2015), extensibility, flexibility, integratability, interoperability, interchangeability, modularity, portability and replaceability.

- *Extensibility* of an open system is understood as its ability to add new components, subsystems, or systems, as well as new capabilities to a system.

- *Flexibility* means that a given system, depending on the current requirements, can be reconfigured, and modified to varying situations.
- *Integratability* of a system means that it can form, coordinate, or incorporate into a larger, functioning whole.
- *Interchangeability* means that a given system or a part of it can be replaced with another one without losing the basic system properties and features.
- *Interoperability* is the ability of connected, autonomous, flexible coupled and usually heterogeneous systems to cooperate and to exchange streams of data, services, material, and energy to and from other systems, while continuing their own way of operation.
- *Modularity* of a given system means that it is built of functional blocks, separating the system's capacities into modules.
- *Portability* is the ability to be moved from one environment to another.
- *Replaceability* is understood as the ability of a system, component, or person to take the place of another, especially as a substitute or successor.

According to the ESoS definition, the subsystems included in the ESoS are heterogeneous and autonomous, while the entire ESoS must achieve objectives that are not the same as those of any of the subsystems. Therefore, each ESoS must contain an additional *metasystem* that fulfils a management or governance role in relation to all subsystems of ESoS. Therefore, the design, instalment, operation, and transformation of metasystem play a key role in architecting reliable ESoS. The metasystem is comprised of autonomous embedded complex systems, that can diversify in technology, context, operation, geography, and conceptual frame.

There are four elements essential to understanding this approach, including the metasystem construct, the nine metasystem functions, the corresponding ten communication channels, and the relationship of the metasystem to the subsystems. The *metasystem construct* brings several important considerations, including (Keatin and Katina, 2016):

- It operates at a logical level beyond the system, subsystems, and entities that it must integrate,
- It has been conceptually grounded in the foundations of Systems Theory (axioms and propositions governing system integration and coordination) and Management Cybernetics (design of the communication and control for effective system organization),
- It has a set of interrelated functions, which only specify 'what' must be achieved for continuing system existence, not specifying 'how' those functions are to be achieved,
- Its functions must be minimally performed if a system is to remain viable – this does not preclude the possibility that a system may be poorly performing, yet continue its existence,

- It can be purposefully designed, executed, and maintained, or left to its own unstructured development.

The metasystem construct is a basis of ESoS and determines its reliability. The metasystem is the 'governor' in a cybernetic sense of providing control for a system. This type of control is essential to ensure a system maintains the stability of performance in situations external environmental changes and turbulences. Control generated by the metasystem is achieved in conjunction with three primary roles (Keating *et al.,* 2014), including:

- Communication – organization of the flow, transduction, and processing of information internal and external to the system, that provides for consistency in decisions, activities, interpretations, and knowledge creation made with respect to the system.
- Coordination – providing for interactions between constituent entities within the system, and between the system and external entities to avoid undesirable instabilities and disturbances.
- Integration – ensuring continuous maintenance of system integrity. This requires a dynamic balance between autonomy of constituent entities and the integration of those entities to form a coherent whole. This balance produces the system identity and uniqueness that exists beyond the identities of the individual constituents.

The second element of metasystem involves the *governance functions*, including four primary functions and five associated sub-functions. These are the following functions: (Keating *et al.,* 2014):

- Policy and identity – maintain and defines the balance between current and future state of an organization from two perspectives:
  - System perspective – focused on the specific system context within which the metasystem is embedded.
  - Strategic perspective – focused on monitoring of the system performance indicators at a strategic level, identifying system level performance that meets, exceeds, or fails to meet established performance expectations.
- System development – concentrates on the long-range development of the system to ensure future viability thanks:
  - Environmental monitoring – supervision of the environment for trends, patterns, or events.
  - Learning and transformation – correction of design imperfections in the metasystem functions and communication channels and planning for transformation of the metasystem.
- System operations – the current execution of the metasystem to ensure that the overall system maintains required performance levels.

  - Operational performance – monitors system performance to identify and assess abnormal conditions, exceeded thresholds, or anomalies.
- Information and communications – design, establishes, and maintains the flow of information through communication channels, and consistent interpretation of exchanges necessary to fulfil metasystem functions.

The main metasystem functions are interrelated, thus, the execution of the functions as well as communication channels determines the level of governance effectiveness and finally system performance. These channels provide for the flow of information and consistency in interpretation for exchanges within the metasystem and between the metasystem and external entities. Table 1 shows a brief listing of the communication channels, their primary metasystem function responsibility, and the role they play in metasystem execution.

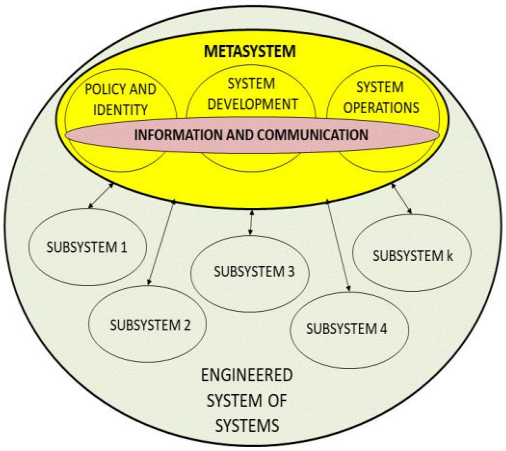
Table 1. *Communication channels of the metasystem.*

Function	Sub-functions	Description of the function's role
F1. Policy and identity	F1.1 Command	Provides non-negotiable direction to the metasystem and governed systems
	F1.2 Control	Provides for examination of system decisions, actions, and interpretations for consistency with system purpose and identity
	F1.3 Emergency	Provides redundancies of all channels when the integrity of the system is threatened and compels instant alert to crisis or potentially catastrophic situations for the system
F2. System development	F2.1 Environmental monitoring	Provides design for sensing to monitor critical aspects of the external environment and identifies environmental patterns, activities, or events with system implications
	F2.2 Learning and transformation	Provides detection and correction of error within the metasystem as well as governed systems, focused on system design issues as opposed to execution issues
F3. System operations	F3.1 Resource management	Determines and allocates the resources (manpower, material, money, methods, time, information, support) to governed systems and defines performance levels (e.g. productivity), responsibility, and accountability for governed systems
	F3.2 Operations management	Provides for the routine interface concerned with near term operational focus; concentrated on providing direction for system production of value (products, services, processes, information) consumed external to the system
	F3.3 Audit	Provides routine and sporadic feedback concerning operational performance as well as investigation and reporting on problematic performance issues within the system
F4. Information and communication	F4.1 Coordination	Provides for metasystem and governed systems balance and stability as well as ensures design and achievement (through execution) of design: • ensuring that decisions and actions necessary to prevent disturbances are shared within the metasystem and governed systems, and • sharing of information within the system necessary to coordinate activities
	F4.2 Informing	Provides for flow and access to routine information within the metasystem or between the metasystem and governed systems

Source: *Authors' own composition based on Keating and Katina, 2016.*

Figure 1 shows an example of the functional structure of an Engineered System of Systems. As can be seen from this diagram, the metasystem plays a dominant role in the management of the entire complex system of systems and has direct relationships with each of the subsystems that make up the entire ESoS. However, the coherence of the management functions in the metasystem is ensured by the F4 function, information, and communication. This functional structure of the ESoS ensures that even very complex systems, such as those found in global supply networks, can be fully controlled, and governed.

Figure 1. *An example of the functional structure of an Engineered System of Systems.*



Source: *Authors' own composition based on Bukowski, 2019.*

Given the characteristic features of modern logistics networks, which were briefly discussed in Section 1 (Introduction), we believe that the application of the ESoS model to describe complex logistics organizations is fully justified.

3. From High Reliable Organization Concept to the Idea of Resilient Enterprise

The starting point for the idea of a Reliable and Resilient Logistics Organization (RRLO) is the well-known High Reliability Organization (HRO) concept. A High Reliability Organization is an organization which has succeeded in avoiding catastrophes in an environment where normal accidents can be expected with significant probability. This concept is based on the Normal Accident Theory (NAT) developed by Charles Perrow in 1984 and its main idea is that accidents are inevitable in complex organizations that operate high-risk technologies. Perrow argued that there are certain defining characteristics, which make the occurrence of accidents in such organizations inevitable, namely tight coupling of individual parts of the organization and interactive complexity. This coupling refers to the degree of interdependence

among a system's components (e.g., people, technology, procedures), whilst interactive complexity refers to the extent to which the interactions among the system's components are often unpredictable and invisible. Consequently, because of interdependency, a failure that occurs in one part of the system can quickly disseminate to other parts of the system (the so-called cascading failures). It means that there is imperfect knowledge (due to the system's complexity) and insufficient time (due to the tight coupling of operations) to fully understand, intervene and contain potential failures (Perrow, 1984).

Traditionally, HRO user have relied on accident statistics as evidence that an organization meets the 'high reliability' criterion of almost *error-free performance*. However, these statistics have been criticized as lacking objectivity and confounding reliability with safety and security. HRO characteristics are often discussed in the context of major accidents and are used to highlight the operational safety standards that organizations should try to follow. The MIIB report (2008) recommended that the following factors should be considered to achieve a High Reliability Organization:

- An explicit definition and understanding of roles and responsibilities as well as assuring competence in these roles.
- Enabling front line staff to diagnose and respond to incidents through effective control procedures, design, and alarm systems.
- Providing appropriate personnel and shift work arrangements to control major accident threats.
- Providing suitable training, experience and competence assurance systems for staff engaging in safety-critical activities.
- Auditing and operational supervision of contractors' abilities to supply and maintain high integrity equipment.
- Providing proper arrangements for the effective supervision of control staff.
- Setting and implementing appropriate standards for safe and effective communication at shifts and handovers.
- Assurance of effective standardized procedures for most important maintenance, testing and operational activities.
- Ensuring that management of changes is addressed effectively and includes organizational, procedural as well as equipment changes.

In summary, research in area of HRO has revealed several important processes that play an essential role in the safety performance of these organizations. However, this concept has also raised several vital questions, predominantly regarding the transferability and underlying mechanisms of HRO processes, as well as their financial justification (Lekka, 2011). Table 2 shows the main features and processes characteristic for a High Reliability Organization compiled from literature data.

Table 2. *Main features and processes characteristic for a High Reliability Organization.*

Features and processes type	Examples of requirements for features and processes
Typical attributes of organization	• Interactive complexity (interaction among system components is unpredictable and/or invisible), • Tight coupling (high degree of interdependence among a system's components including people, equipment and procedures), • Potentially catastrophic consequences of failure.
Containment of unexpected events	• Redundancy (having in place back-up systems in the event of failures and cross-checking of important decisions), • Deference to expertise making safety-related decisions in emergencies, • Fluctuation between hierarchical and flat (decentralized) organizational structures, • Investment in training and technical competence, • Well-defined procedures for all possible unexpected events.
Anticipation of potential failures	• Engagement with front line staff in order to obtain 'the bigger picture' of operations (sensitivity to operations), • Attentiveness to minor disturbances and deviations from the normal state and using incidents and near misses as indicators of a system's reliability (preoccupation with failure), • Systematic collection and analysis of all warning signals and avoiding to making assumptions regarding only the nature of failures (reluctance to simplify).
Safety culture	• Open reporting systems for near misses and accidents without fear of punishment, • Follow-up of accident investigation outcomes by implementing corrective actions, • Empowering staff to abandon work on safety grounds, • Fostering a sense of personal accountability for safety.
Learning orientation	• Continuous technical training, • Systematic analysis of incidents (to identify their root causes) and accident types or trends within the organization, • Open communication of accident investigation outcomes, • Updating procedures in line with the organizational knowledge base.
Mindful leadership	• Proactive commissions of audits to identify problems in the system, • Bottom-up communication of 'bad news', • Engagement with front line employee through site visits, • Investment of resources in safety management and the ability to balance profits with safety.

Source: *Authors' own composition based on Lekka, 2011.*

The HRO concept has worked well in stable environments and in situations of predictable change. However, it failed in turbulent environments and when the changes taking place were unpredictable. The answer to this challenge was the concept of *resilient enterprise*.

The term 'resilience' has been used in professional literature for over 20 years (Hollnagel *et al.*, 2006; Mallak, 1999; Sutcliffe, 2003; Scott *et al.*, 2006; Vogus and Sutcliffe, 2007). According to Vogus and Sutcliffe (2007), *organizational resilience*

is defined as *the maintenance of positive adjustment under challenging conditions such that the organization emerges from those conditions strengthened and more resourceful*. Thus, creating organizational resilience is associated with the people and management concerns. From systemic perspective, we can define an enterprise as a complex system consisting of technology and information infrastructure, processes, and people, with the goal of producing goods and/or services using physical, financial, and human resources. Gallopin (2006) defines *enterprise resilience as an enterprise's adaptive capacity and its ability to cope with, adapt to and recover after a disruption.* He also states that to decrease the susceptibility to potential disruption risks enterprises are required to reduce the complexity of their infrastructures. Achieving these goals and assessing the vulnerabilities embedded within the enterprise elements requires understanding the interrelationships and interdependencies between the business processes, information, and the supporting technologies within and outside the enterprise.

Sheffi and Rice (2005) describe the process of creating a resilient enterprise as a strategic initiative that changes the way an enterprise operates and that increases its competitiveness. They suggest that enterprise resilience can be achieved by reducing its vulnerability to disruption risks, by creating infrastructures redundancy, and by increasing processes flexibility. The ability to bounce-back when a disruption occurs can be defined by the adaptive capacity of the enterprise and its redundancy or increasing flexibility. The authors also describe resilience as a function of the enterprise competitive position and the responsiveness of its supply chain. *Disruptive events* are defined as random events caused by internal and external factors affecting a system as well as generate a short- or long-term negative impact on the performance of the system.

Resilience of an enterprise can be measured by the level of its vulnerability to a specific risk (Berkes, 2007). *Vulnerability* is defined as being at risk with a significant probability of having disruptions (Christopfer and Peck, 2004). Thus, reducing the vulnerabilities has positive impact on the resilience of any system by decreasing the likelihood of a disruption and increasing the ability to bounce back from a disruption. The measure of vulnerability is the duplet – the probability of the occurrence of a disruption and the value of its consequences (Sheffi and Rice, 2005).

Adaptive capacity is a concept that has been strongly associated with resilience (Dalziell and McManus, 2004; Fiksel, 2006; Gallopin, 2006; Stevenson and Spring, 2007). In order to improve resilience, the adaptive capacity of an enterprise should be increased both before and after a problem is detected. Stevenson and Spring (2007) define adaptive capacity as the system's response to the changes in its environment. The adaptive capacity of a system can be increased by designing, planning, and building flexibility in organization. *Flexibility* can be defined as the ability of an enterprise to adapt to the changing requirements of its environment and its stakeholders with minimum time and effort. Fiksel (2006) describes flexibility as a

major system characteristic that contributes to resilience as a system's ability to bounce back from disruptions and disasters.

The adaptive capacity has been often related to concepts of *robustness, agility, and adaptability* (Christopfer and Peck, 2004; Fricke and Schulz, 2005; Walker *et al.*, 2004). Robustness characterizes an ability to be resistant to changing environments, and agility indicates an ability to change rapidly, whereas adaptability shows an ability to adjust towards changing environments while providing the intended functionality under varying operating conditions (Fricke and Schulz, 2005). Agility has been used in conjunction with flexibility as an important attribute of resilience (Christopfer and Peck, 2009) as a system's ability to respond quickly to changes in an uncertain and changing environment.

Information and *connectivity* can be seen as next essential elements of resilience. Creating enterprise resilience relies on perceiving environmental change rapidly and implementing adaptive responses early. Effective use of enterprise information systems can improve decision-making abilities of the organization that results in increased flexibility, agility, and adaptability, supporting attributes of resilience (Fiksel, 2006; Haimes *et al.*, 2008; Szczepańska-Woszczyna, 2018).

Summarizing we can define enterprise resilience as a function of robustness, flexibility, agility, adaptability, and redundancy. Alignment of business processes and information technology is also an enabling factor for enterprise resilience which requires simple and manageable enterprise architecture and efficient enterprise integration.

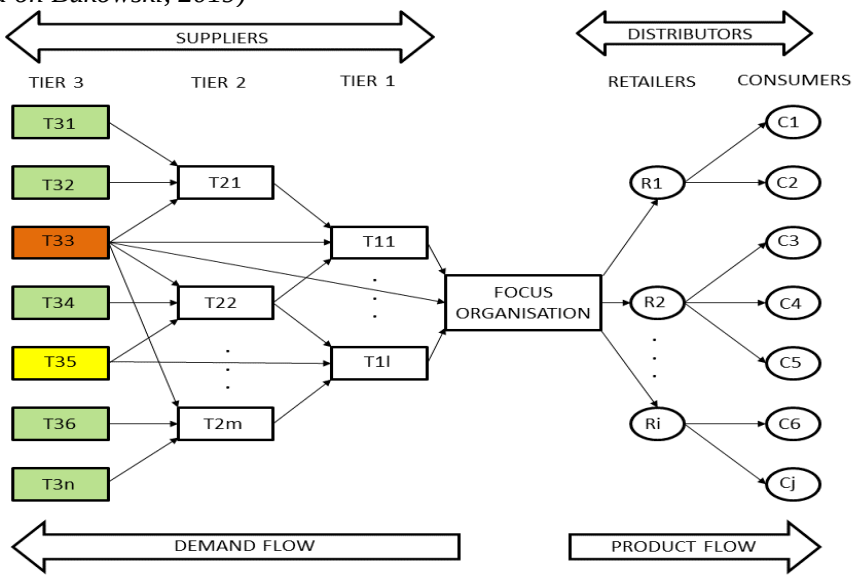
4. The Concept of Reliable and Resilient Logistics Organization

Typical representatives of complex organizations in practice are global supply chains and networks. The issue of risk in logistics organizations has been addressed in research work worldwide and especially in recent years (Hys, 2014; Jagoda *et al.*, 2020; Kabus *et al.*, 2020; Kulińska *et al.*, 2020; Pakurar *et al.*, 2020). For complex products such as cars, which feature multiple goods, technologies, and processes, the supply chain becomes very complicated. The simplified logistics supply chain diagram for an automotive company is shown in Figure 2, which illustrates the complexity of the chain, spanning from customers back through multiple levels and suppliers' tiers. The focus organization divides the entire supply chain into supply part (raw materials, parts, and assemblies) and distribution part (finished goods).

Supplier network includes lot of firms that provide items ranging from raw materials, such as steel and plastics, to complex assemblies and subassemblies, such as transmissions, brakes, and engines (Sheffi, 2016). Participants in a supply chain (suppliers, focus organization, distributors and consumers) should work closely together, which requires the constant exchange of information and complete trust

between them. Therefore, organizations are effectively forming new types of relationships called partnerships or alliances that require sharing of assets and resources.

Figure 2. *The simplified logistics supply chain diagram for an automotive company (based on Bukowski, 2019)*



Source: *Authors' own composition.*

In addition, the environment in which supply chains operate, and in particular the risks associated with the complexity of relationships and the unpredictability of certain developments and changes, plays a very important role in the functioning of supply chains. Thus, *ensuring the continuous and efficient operation of logistics organizations*, particularly those with a global scale, requires effective and efficient risk, reliability, and resilience governance approach.

The concept of Reliable and Resilient Logistics Organization should be an adequate response to these problems. In developing it, the authors relied on the idea of *'idealized design'* proposed by a team led by Ackoff *et al.* (2006) and a document developed by the International Risk Governance Center called *IRGC Risk Governance Framework* (IRGC, 2017). In this work the concept of risk refers to uncertainty about and the severity of the consequences of an activity or event with respect to something that humans value. Uncertainty can include the type of consequences, the likelihood of these occurring (usually expressed in probabilities), the severity of the consequences or the time or location where and when these consequences may occur (SRA, 2015). This definition accommodates both desirable (positive) and undesirable (negative) outcomes, but most organizations focus only on the negative outcomes. In today's logistics organizations, risks and systems are deeply inter-connected as well as increasingly systemic, and can seriously threaten the functionality of complex

systems, like logistics organizations. Such systemic risks cannot be managed through the actions of a single agent, but require the involvement of different stakeholders, including governments, industry, and members of civil society. Some systemic risks can even have global impacts (e.g., pandemic), requiring coordinated management approaches at local, regional, national, and international levels. In this sense, the management of such systems and organizations is called 'governance'.

Governance refers to the actions, processes, traditions, and institutions by which authority is exercised and collective decisions are taken and implemented. *Risk governance* applies the principles of governance to the identification, assessment, management, evaluation, and communication of risks in the context of plural values and distributed authority. It includes all important actors involved, considering their rules, conventions, and processes (IRGC, 2017).

The IRGC Framework is a comprehensive approach to help understand, analyze and manage important risk issues for which there can be deficits in risk governance structures and processes. The Framework comprises four interlinked elements, with three cross-cutting aspects:

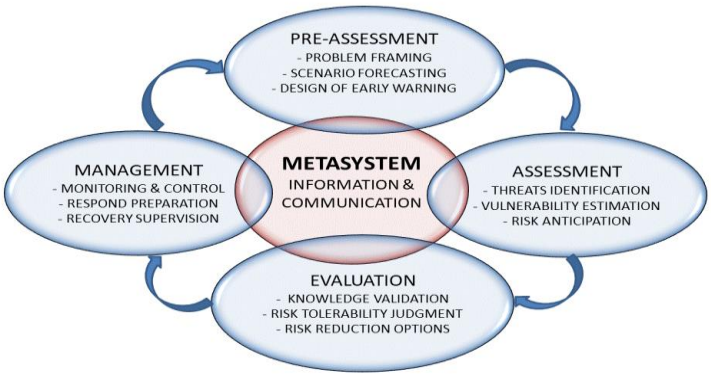
- Pre-assessment – identification and framing; setting the boundaries of the risk or system.
- Appraisal – assessing the technical and perceived causes and consequences of the risk.
- Characterization and evaluation – making a judgment about the risk and the need to manage it.
- Management – deciding on and implementing risk management options.
- Cross-cutting aspects – communicating, engaging with stakeholders, considering the context.

Based on these universal assumptions, the authors propose a general concept of Reliable and Resilient Organization (RRO), the idea of which is shown in Figure 3. The RRO was assumed to be a System of Systems consisting of four core systems and one metasystem. The core of the system is the *meta-system*, whose role is to ensure continuous and uninterrupted communication between the individual systems through reliable information flow. More detailed requirements for the metasystem are summarized in Table 1.

Pre-assessment captures problem framing, describing existing indicators, routines and standards which may help limit what is to be addressed as the risky scenarios, as well as the manner in which it should be addressed and analyze. It is particularly important to develop effective early warning signals that warn of both expected and unexpected 'Black Swan' type threats (surprising extreme events also called 'unknown-unknown'). The *Assessment* system is responsible for performing a full identification of existing threats and hazards, assessing the organization's vulnerability to types of these dangers

and, on this basis, anticipating the risk of losing business continuity. *Evaluation* is primarily concerned with verifying and validating the knowledge possessed by decision-makers, which is the basis for the implementation of management processes.

Figure 3. *Visual presentation of the Reliable and Resilient Organization concept*



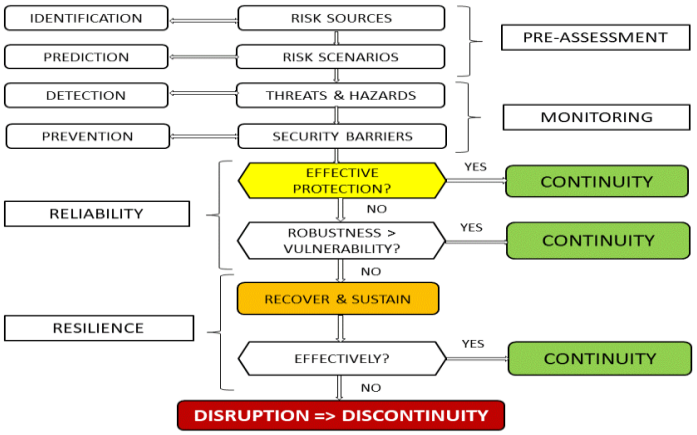
Source: *Authors' own composition.*

Based on this knowledge, a risk severity assessment should be carried out on a three-stage scale, acceptable (risk reduction is considered unnecessary), tolerable (risk can be pursued) or intolerable (risk source must be avoided). In addition, risk reduction options should be developed, and the most favorable ones selected. Effective RRO *management* mainly boils down to continuous monitoring and control of any changes and early warning signals. On this basis, appropriate risk response options should be prepared (e.g., based on the Resilience-Based Maintenance method, see Bukowski and Werbińska 2020). If the situation requires recovery to restore the continuity of the organization, recovery supervision is necessary. We have called the application of the general concept of RRO in supply chains *Reliable and Resilient Logistics Organization (RRLO)* and for this application area we propose a framework presented as an algorithmic diagram in Figure 4.

The process of governing RRLO to ensure operational continuity begins in Pre-assessment with the identification of potential sources of risk. The identified and described risk sources form the basis for the prediction of possible risk scenarios. On this basis, a monitoring system should be developed that tracks and detects specific threats as well as hazards occurring during the organization's operation (also early warning signals of possible threats). A properly designed system should also be equipped with security barriers, whose role is to prevent the possible negative effects of hazards. Monitoring also checks the effectiveness of these barriers. If the barriers prove ineffective (e.g., if the threat was fully unpredictable, or its scale exceeded the capabilities of the protection barriers) the continuity of the organization's operations is determined by its reliability, i.e., meeting the condition that its robustness is greater than vulnerability. If this condition is not met, it is the organization's resilience, i.e.,

its ability to bounce back quickly and maintain the required level of performance, that determines its future. If the level of resilience is satisfactory, the operational continuity of the organization is maintained; if it is not, disruption occurs, and the continuity of the organization is lost.

Figure 4. *Algorithm of a framework for creating Reliable and Resilient Logistics Organizations*



Source: *Authors' own composition.*

Each case of 'disruption' should be thoroughly investigated and add to the organization's baseline knowledge. A modern organization should be able to learn and adapt, so modification measures to improve the organization's reliability and resilience should be implemented as soon as possible. This process - learning and adaptation - should be continuous and never-ending.

5. Summary and Concluding Comments

Contemporary logistics organizations are characterized by a topology of complex network structures that perform specific functions, consisting of moving in space and time, as well as storing goods in an efficient and effective manner, in a changing and uncertain environment with possible disturbances and threats. Increasingly, the activities of logistics organizations span the globe, which brings with it challenges and hitherto unknown dangers. Therefore, the need of the hour is to develop methods to create such organizations, considering both predictable changes and threats, and those that so far logistics managers have not had to deal with and are even difficult to imagine.

The aim of this work was to synthesize current knowledge in the field of complex logistic organizations governance, and on this background to present a new concept of reliable product delivery assurance. The concept of the Reliable and Resilient Logistics Organization (RRLO) should be an adequate response to these problems.

The authors proposed to assume that each complex logistics organization can be modelled as a System of Systems (SoS) consisting of four core systems and one metasystem. The core of SoS is a *meta-system*, whose role is to ensure continuous and uninterrupted communication between the individual systems through reliable information flow. This was followed by an analysis of the advantages and disadvantages of known management concepts for such organizations, namely High Reliability Organization (HRO) and an idea of Resilient Enterprise (RE). Based on this analysis and the authors' own experience, an RRLO concept was proposed that combines the advantages of both concepts and minimizes their weaknesses. In the final part of the article, a framework for the application of the developed concept is presented in the form of an algorithm that can support the practical implementation of the RRLO concept.

We intend to focus further work on detailing the developed algorithm and verifying it on the example of a global logistics organization model. For the description of the organization, we envisage using a multi-agent technique, while for the modelling of threats and disturbances - simulation methods based on generating discrete random events. The next step of our research will be to try to integrate the RRLO concept with the general Risk Governance model and the Resilience-Based Maintenance concept that we have developed in recent years.

References:

Ackoff, R.L., Magidson, J., Addison H.J. 2006. Idealized design: creating an organization's future. Pearson Education LTD.

Berkes, F. 2007. Understanding uncertainty and reducing vulnerability: lessons from resilience thinking. Nat Hazards, 41, 283-295.

Blanchard, B.S. 2015. Logistics Engineering and Management. Pearson Education.

Billaud, S., Daclin, N., Chapurlat, V. 2015. Interoperability as a key concept for the control and evolution of the System of Systems (SoS). International Workshop on Enterprise Interoperability, https://www.researchgate.net/publication/279928616_Interoperability_as_a_Key_Concept_for_the_Control_and_Evolution_of_the_System_of_Systems_SoS.

Bukowski, L. 2016. System of Systems Dependability - Theoretical Models and Applications Examples. Reliability Engineering & System Safety, 151, 76-92.

Bukowski, L. 2019. Reliable, Secure and Resilient Logistics Networks. Delivering products in a risky environment. Springer Nature Switzerland AG 2019, ISBN 978-3-030-00849-9, Hardcover, eBook.

Bukowski, L., Werbińska-Wojciechowska, S. 2021. Using fuzzy logic to support maintenance decisions according to Resilience-Based Maintenance concept, Eksploatacja i Niezawodność. Maintenance and Reliability, 23(2), 294-307. http://doi.org/10.17531/ein.2021.2.9.

Christopher, M., Peck, H. 2004. Building Resilient Supply Chain. International Journal of Logistics Management, 15, 1-13.

Christopher, M., Peck, H. 2009. The Five Principles of Supply Chain Resilience. Logistics Europe, 12, 16-21.

Dalziell, E.P., McManus, S.T. 2004. Resilience, Vulnerability, Adaptive Capacity: Implications for System Performance, International Forum for Engineering Decision Making (IFED). Stoos, Switzerland.

DoD. 2008. Systems Engineering Guide for Systems of Systems. Ver. 1.0. Office of the Deputy under Secretary of Defense for Acquisition, Technology and Logistics. Washington, DC.

Fiksel, J. 2006. Sustainability and Resilience: Toward a Systems Approach. Sustainability: Science, Practice, & Policy, 2, 14-21.

Fricke, E., Schulz, A.P. 2005. Design for Changeability (DfC): Principles to Enable Changes in Systems Throughout Their Entire Lifecycle. Systems Engineering Journal, 8, 342-359.

Gallopin, G.C. 2006. Linkages between vulnerability, resilience, and adaptive capacity. Global Environmental Change, 16, 293-303.

Gudehus, T., Kotzab, H. 2009. Comprehensive Logistics. Springer, Berlin Heidelberg.

Harisson, A., van Hoek, R., Skipworth, H. 2014. Logistics Management and Strategy: Competing through the Supply Chain. Pearson.

Haimes, Y.Y., Crowther, K., Horowitz, B.M. 2008. Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems. Systems Engineering, 11, 287-308.

Hollnagel, E., Woods, D.W., Leveson, N., (Eds.). 2006. Resilience Engineering: Concepts and Precepts. Ashgate, Abingdon, Oxon, GBR.

Hys, K. 2014. Tools and methods used by the Polish leading automotive companies in quality management system. Results of empirical research, Journal of Achievements of Materials and Manufacturing Engineering, Publisher: International OCSCO World Press, 63(1), 30-37.

IRGC. 2017. The IRGC Risk Governance Framework, revised version. Lausanne, EPFL International Risk Governance Center.

Jagoda, A., Kołakowski, T., Marcinkowski J. 2020. Project Teams as a Supply Chain Integration Tool. European Research Studies Journal, 23(1), 176-185.

Jamshidi, M. 2011. System of systems engineering: innovations for the twenty-first century. John Wiley & Sons.

Kabus, J., Miciuła, I., Piersiala, L. 2020. Risk in Supply Chain Management. European Research Studies Journal, 23(4), 467-480.

Keating, C. 2005. Research Foundations for System of Systems Engineering. In: IEEE International Conf. on Systems, Man and Cybernetics. Waikoloa, Hawaii, 2720-2725.

Keating, C., Katina, P. 2016. Complex system governance development: a first-generation methodology. Int. J. System of Systems Engineering, 7, 1/2/3, 43-74.

Keating, C.B., Katina, P.F., Bradley, J.M. 2014. Complex system governance: concept, challenges, and emerging research. International Journal of System of Systems Engineering, 5(3), 263-288.

Kulińska, E., Giera, J., Smaga, K. 2020. Analysis of Risk Factors in an Indirect Distribution Channel. European Research Studies Journal, 23(1), 176-185.

Lasch, R. 2014. Strategisches und operatives Logistikmanagement: Prozess. Springer Gabler, Wiesbaden.

Lekka, C. 2011. High reliability organizations: A review of the literature. RR899 Research Report. http://www.hse.gov.uk/research/rrpdf/rr899.pdf.

Mallak, L. 1999. Toward a Theory of Organizational Resilience. Portland International Conference on Technology and Innovation Management, PICMET, 1, 223.

MIIB. 2008. Major Incident Investigation Board. The Buncefield incident 11 December 2005: The final report of the Major Incident Investigation Board, 1. http://www.buncefieldinvestigation.gov.uk/reports/volume1.pdf.

Nyhuis, P., Wiendal, H.P. 2009. Fundamentals of Production logistics. Theory, Tools and Applications. Springer-Verlag, Berlin Heidelberg.

Pakurár, M., Kun, I.A., Felföldi, J., Vasa, L., Oláh, J. 2020. Integration of Logistics Function and Business Performance. European Research Studies Journal, 23(3), 567-583.

Pfohl, H.C.H. 2016. Logistikmanagement: Konzeption und Funktionen. 3. Auflage. Springer-Verlag, Berlin, Heidelberg.

Perrow, C. 1984. Normal accidents: Living with high-risk technologies. NY, Basic Books.

Scott, M., Sorcinelli, G., Gutierrez, P., Moffatt, C., DesAutels, P. 2006. Conferencexp: An Enabling Technology for Organizational Resilience, in the Transfer and Diffusion of Information Technology for Organizational Resilience. In: Donnellan, B., Larsen T., Levine L.D.J. (Eds.), Boston, Springer, 219-227.

Sheffi, Y. 2016. The Power of Resilience: How the Best Companies Manage the Unexpected. The MIT Press, Cambridge, Massachusetts, London, England.

Sheffi, Y., Rice, J.B.Jr. 2005. A Supply Chain View of the Resilient Enterprise. MIT Sloan Management Review, 47(1), 41-48.

SRA Glossary. 2015. http://www.sra.org/sites/default/files/pdf/SRA-glossary-approved 22 june2015-x.pdf.

Stevenson, M., Spring, M. 2007. Flexibility from a supply chain perspective: definition and review. International Journal of Operations & Production Management, 27.

Sutcliffe, K.M. 2003. Organizing for Resilience. In: Positive Organizational Scholarship, K. S. Cameron, I.E. Dutton, R.E. Quinn, (Eds.), San Francisco, Berrett-Koehler, 94-110.

Szczepańska-Woszczyna, K. 2018. Strategy, corporate culture, structure, and operational processes as the context for the innovativeness of an organization. Foundations of Management, 10(1), 33-44.

Vogus, T.J., Sutcliffe, K.M. 2007. Organizational Resilience: Towards a Theory and Research Agenda. Systems, Man and Cybernetics.

Walker, B., Holling, C.S., Carpenter, S.R., Kinzig A. 2004. Resilience, adaptability, and transformability in social-ecological systems. Ecology and Society, 9(2), 5. http://dx.doi.org/10.5751/es-00650-090205.