Fraunhofer
IML

FRAUNHOFER INSTITUTE FOR MATERIAL FLOW AND LOGISTICS IML

RISK MANAGEMENT OF DISRUPTIVE EVENTS IN SUPPLY CHAINS

MANAGEMENT SUMMARY

Disruptive events and their effects are not a new phenomenon that needs to be considered in the context of risk management. There have always been unforeseeable events with significant impacts and little to no warning time in business practice. However, the development of worldwide value-added structures to move toward global and networked supply chains with closely integrated logistics and value-added processes, has greatly increased the vulnerability of individual supply chains. Longer transport distances, globally distributed supplier and customer structures and reliance on the functioning of tightly synchronised networks are susceptible to massive impact in the event of an unplanned and perhaps even unforeseeable disruption. Increasing political and social uncertainties and the growing number of extreme environmental and weather events due to climate change continue to highlight the importance of disruption risk management [1].

The best possible preparation and response to disruptions, together with the identification of potential dangers and the fastest possible recovery of supply chains affected by disruptions, is therefore an increasingly important area within risk management. The increasing relevance of this particular risk component must also be reflected in company structures, processes and IT systems and in cross-company supply chains. Currently, only about 25% of the companies interviewed in a survey identify, measure and report disruptive events on a company-wide basis and in integrated systems [2].

In many cases, current technologies to support the management of disruptive events, such as artificial intelligence, block chain or simulation, are already available and integrated in software solutions. However, many companies have still not begun adapting processes and structures or ensuring that employees have the organisational and technological skills to be able to realise the potential that technology can make possible. On the other hand certain individual companies are already preparing the entire supply chain for disruptive shocks in the best possible way through modern IT, customised internal organisation and collaboration with value creation partners.

In preparing this white paper, technical experts and decision-makers from industry and trade together with external knowledge carriers were involved in order to obtain the most comprehensive and cross-sector view possible on the topic of disruptive risks. Based on these interviews, four areas of activity were identified - risk awareness, transparency, flexibility and cooperation - for companies and supply chains, in which current shortfalls in the instruments, methods and measures used were the focus. The need to support employees, processes and functionalities have been identified in both the preparatory proactive and reactive measures and solutions. With regard to these areas of activity, technology-based approaches and solutions are presented, which are intended to provide support while getting to grips with the existing challenges.

WHITEPAPER

RISK MANAGEMENT OF DISRUPTIVE EVENTS IN SUPPLY CHAINS

CONTENTS

Management Summary 2
Motivation and Introduction 4
Shortfalls and Required Action for the Management of Disruptive Events 6
- Shortfalls of Current Instruments in Risk Management 6
- Action Required for Risk Management 9

New Technologies and Methods 12
- Current Trends and Developments in Supply Chain Management 12
- Technologies for Dealing with future Disruptive Events 12
- Methods and Solutions for Dealing with Disruptive Events 14
- Assessing the Availability of Solutions and Technologies and the Current Action Required 17

Conclusion and Outlook 18
References 19

AUTHORS
Lorenz Kiebler, Fraunhofer IML
Dietmar Ebel, Fraunhofer IML
Philipp Klink, Fraunhofer IML
Saskia Sardesai, Fraunhofer IML

CONTACT
Fraunhofer Institute for Material Flow and Logistics IML
Joseph-von-Fraunhofer-Str. 2–4
44227 Dortmund

INSTITUTE MANAGEMENT
Prof. Dr.-Ing. Uwe Clausen
Prof. Dr. Michael Henke
Prof. Dr. Michael ten Hompel (Managing Director)

IMAGE LICENCE - COVER PICTURE AND INNER SECTION
© Anton Balazh, lassedesignen, Edelweiss, Maksim Pasko - Fotolia

COVER, LAYOUT UND TYPESETTING
Sabrina Peters, Fraunhofer IML

DOI
10.24406/iml-n-599828

© Fraunhofer IML, Dortmund 2020

This white paper was issued with sponsorship from Oracle Germany.

MOTIVATION AND INTRODUCTION

Current developments such as globalisation, the individualisation of customer requirements and products as well as generally increasing environmental dynamics are causing supply chains to become increasingly complex. Supply chains span various countries, use closely synchronised transport and delivery windows and reduce inventories, costs and lead times by strengthening collaboration between the partners involved. However, if this fine-tuned collaboration is disrupted by unforeseen events, the impact is even more significant if there is inadequate preparation. In addition, the **susceptibility of supply chains to disruptions fundamentally increases** as networks and environmental volatility progress [3].

As a result of the various trends, the environment of global supply chains is developing towards a less deterministic and increasingly unpredictable setting, which therefore cannot be planned for [4], and can be summarised by the abbreviation **VUCA**: The combination of volatility, uncertainty, complexity and ambiguity means conventional risk management instruments need to be further expanded. Especially in environments that are characterized by VUCA attributes, there are many risks for supply chains. Risks generally describe events that cannot be predicted with certainty and deviations from planned results, which can be specified by the cause of the risk, a probability of occurrence and the effects of damage [5, 6]. In principle, positive opportunities that cannot be predicted with certainty can also be considered as risks. In the general understanding of the term ‚risk' and in terms of management, however, the term primarily refers to **negative loss events** [3,7], hence this meaning of the word is also used in this white paper. With regard to supply chains, risks negatively influence the flow of information, materials, end products and also financial flows between raw material suppliers and end customers in a value chain [3].

In general, supply chain risks - as a subgroup of all existing risks of a company - can be divided into **internal supply chain risks** for material, financial or information flows such as production, liquidity or IT risks, and **external supply chain risks** such as political, social or market-related events and risks from natural disasters or general environmental events [8, 9]. Risks are highly relevant in the context of supply chain management, since any unplanned failure in one stage of the value chain can affect the entire supply chain and, in the worst case, bring it to a standstill [10]. For 2019, a survey [2] identified IT failures, storms, cyber risks, and potential future terrorist acts or fire hazards as the main reasons for supply chain disruptions with major consequences. What all these events have in common is that they result from non-deterministic, **disruptive events**, which mostly could not be predicted or could only be predicted in the short term.

Disruptive events and the risks resulting from these can be distinguished from **operating risks** on the basis of their probability of occurrence and their impact [11]. In most cases, disruptive events are external in nature and have very low probabilities of occurrence that are difficult to estimate. If they do occur, the consequences are more serious than those of operational risks - such as fluctuations in demand or fluctuations in production times - as shown in Figure 1. [3, 12]

The increasing awareness of the **vulnerability of global value networks to disruptive events** has led to the introduction of a structured risk assessment for supply chains at a corporate and management level. This Supply Chain Risk Management (SCRM) focuses on the identification, evaluation and control of threats and events that threaten companies involved in supply chains, transport routes, information flows or financial aspects of cooperative collaboration.

The importance of managing disruptive risks for a company depends primarily on the scope and globality of supplier and customer relationships. Even small, locally sourcing companies can be affected by disruptive events, but the vulnerabilities of deeply and broadly integrated supply chains as well as global supply chains are increasing dramatically.

In order to create a supply chain in which deviations from plans and disruptions are identified as early as possible, cushioned by countermeasures and compensated by flexible adjustments, both classic methods of risk management and new IT solutions made possible by progressive digitisation can be used. A **resilient supply chain** of this nature, which can return as quickly as possible to the original or a desired and possibly even more ideal state after a disruption [3, 11, 13], implies a high degree of **agility** in reacting to unforeseen events or deviations from the plan [13].

To ascertain the current status and future potential for risk management of disruptive events in supply chains, in the context of this white paper interviews were conducted with various experts and managers from different industries as well as with external scientists, professors and consultants. The findings, assessments and contents of these interviews have been taken into account when developing the fields of action and in the selection of the solution technologies presented. The remaining necessary actions and an assessment of the availability of current and future technologies are at the end of the white paper.

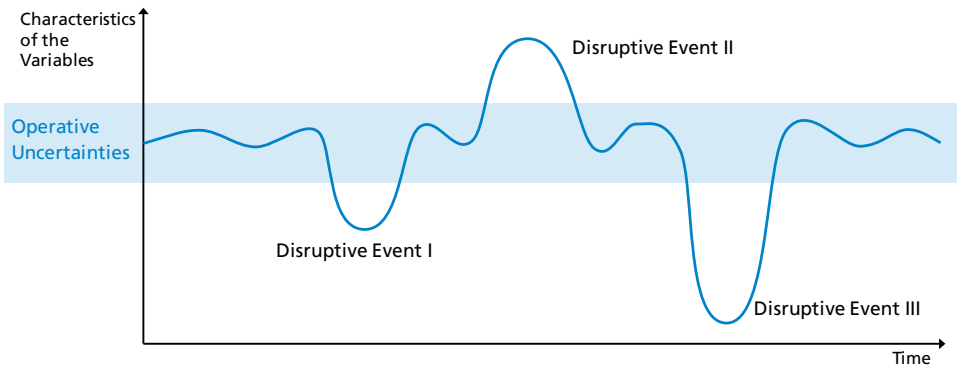

Figure 1: Distinguishing between disruptive and operational risks [11]

SHORTFALLS AND REQUIRED ACTION FOR THE MANAGEMENT OF DISRUPTIVE EVENTS

The capability for managing disruptions within a supply chain can be divided into four different phases before, during and after a disruptive event (see figure 2). In the first phase of **readiness**, the relatively undisturbed supply chain can be proactively prepared for future disruptions. With these disruptions in particular, there is often a variable, short advance warning time at least for parts of the supply chain, which could be used for short-term preparations [11]. Disruptive events cover both expected risks (the expected unexpected) such as earthquakes in vulnerable regions or hurricanes during the Atlantic hurricane season, as well as unexpected risks (the unexpected unexpected) like global pandemics, terrorist attacks, or fires. While proactive preparation for fundamentally expected disruptive disturbances is possible, the preparation for unexpected disruptions is not instantly possible.

At the moment a disruption actually happens, the **reaction phase** begins, in which control is (re-)gained and further damage should be prevented if possible. After the initial disruption and its consequences have been overcome, the **recovery phase** begins, which is intended to make up for and compensate for the accumulated backlogs or consequences in the best possible way. Ideally, the original or even a higher final level across the entire supply chain can ultimately be achieved in the **growth phase.** [3, 14] In the following sections, currently used risk management instruments for disruptive events in supply chains are examined for potential shortfalls in order to subsequently identify the corresponding needs for action.

SHORTFALLS OF CURRENT INSTRUMENTS IN RISK MANAGEMENT

The instruments currently used for risk management can be divided into proactive instruments for preparing a supply chain for disruptions in the readiness phase and reactive instruments specifically for gaining control in the reaction and recovery phase. Depending on the sector and the size of the company, it is apparent that the instruments used can vary considerably. The proactive measures in the readiness phase should ensure a general increase in the resilience of a supply chain, the earliest possible identification of risks and the preparation of a rapid and targeted risk response in the event of damage.

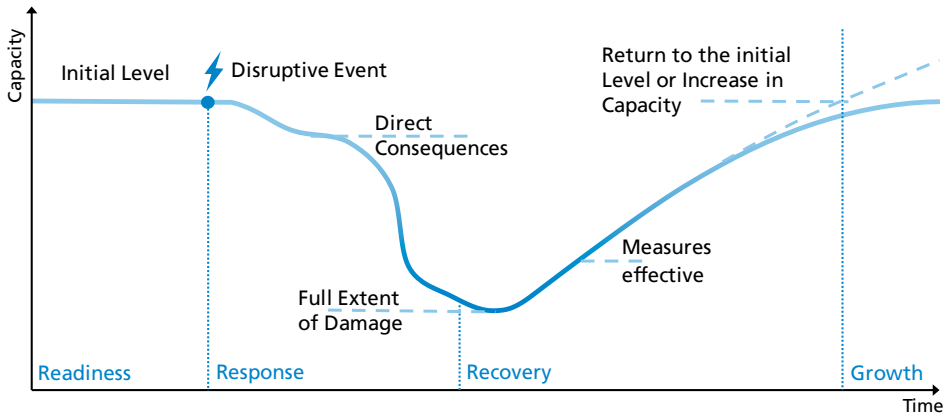

Figure 2: Phases of a resilient supply chain [3, 11, 15]

At present, these risk reactions and the technical support thereof are primarily **organised at a company level,** as the collaboration between the value-added partners in this area is often **insufficiently prepared** and the **technological support for this is inadequate**.

The systematic identification of potential disruptions in the supply chains takes place at different intensities and degrees of standardisation. Many of the surveyed companies in various sectors turn to external information services for information and trend analysis to be able to identify future changes in demand or existing risks as early as possible. Both environmental risks and the effects of risks on demand or supply chains are taken into consideration. In principle, detection and identification is known to be generally associated with many risks but many companies do not make optimal use of the early warning time due to **a lack of awareness of risks, a lack of transparency and a lack of instruments** In some cases they are **unable to identify specific risks promptly.**

»*Fukushima, earthquakes, volcanic eruptions, coronavirus: these affect you. And then it's just a question of how fast and how hard you get hit, and that depends on proactive risk management. In any case, you have to deal with it and you need reactive organisation.*«

Dr. Stefan Geraedts, Director Logistics, Behr-Hella Thermocontrol GmbH

The proactive definition of action plans is intended to ensure that the response phase follows the risk event as quickly as possible in terms of supply chain agility. Due to **a lack of preparation of the measures necessary** to achieve control or to reduce damage, these measures are often uncoordinated, delayed and, in the worst case, can even be ineffective. This comprehensive preparation is much more distinct in larger companies due to various disruptive risks they have experienced in the past and the required capacities which smaller and newer companies do not have. Even the preparatory measures relating to the ability to act in the event of a crisis, for example the **regulation** of **authorities** and **responsibilities within corporate governance**, are often not adapted to all possible risks and are not organised in a structured manner. It is only with such organisational preparation within corporate governance and the rapid formation of a task force that specific risk responses can be decided and implemented quickly and precisely.

The reactive instruments are used immediately after the disruption has occurred or after the early warning - which is only possible to a limited extent - in order to stabilise the supply chain and control the disruptions in the direct response and recovery phases. After an identification as close to real time as possible, the effects on the own supply chain would have to be analysed and the most effective measures would have to be selected and implemented.

»*What can be adapted in any case is a ‚real time' logging, namely a real-time information transfer for the supply chain. We need more transparency regarding where our parts are in the material flow. We need to create an event management system that tells us the relevant events about these real-time events on the transport route.*«

Supplier Manager, Automotive Manufacturer

In complex supply networks, the ability to react as quickly and effectively as possible in terms of cost and benefit to disruption-related, dynamic bottlenecks is already an essential part of operating business. As a result, international corporations with wide-reaching, global supply chains and complex, closely synchronized supply chains are already using IT tools for complexity management in their day-to-day planning, such as special plans or the use of previously planned alternatives and redundancies. Companies with less wide-reaching and less deeply integrated supply chains are often **not prepared for dynamic responses** in terms of software and methods, which can have negative time, financial and organisational effects.

»In the automotive industry we are used to dealing with complexity and also with global networking. This might distinguish us from other industries or even from other companies.«

Dr. Dirk Dreher, Head of Logistics Planning, BMW Group

For smaller companies that are less closely integrated into more vulnerable global supply chains, the importance of structured risk management of disruptive events often only becomes apparent when such a situation with major effects on the company first arises. The **internal company core data** is often not structured in such a way that allows for the analyses and information requirements that are actually necessary. For example, although central contact details of suppliers or customers are often maintained for invoicing and contact purposes, the geographical distribution of locations or origins of goods behind these sales offices or company headquarters are not recorded in a structured way.

Therefore it is very difficult to quickly analyse the effects of disruptions on the company's own supply chain. This cooperation with customers and suppliers, which is necessary in many cases, shows weaknesses due to **unregulated communication channels and systems** as well as challenges with regard to **data sovereignty and trust.** In the event of an incident, information is often transmitted late or only in batches, depending on how the risks are assessed and available capacities. Often, out of fear of misuse of the data provided, **only the immediately essential data is provided.** In good partnerships between companies, however, this communication goes far beyond these areas.

Companies of all sizes also rely on external sources of information, forecasts and assessments for risk identification in the readiness phase as well as in the specific response and recovery phase. The comprehensive monitoring of the various sources of information and the presentation of the vulnerabilities of the supply chain is often **not structured** and **not supported by the system in terms of processes.**

»We are well versed in our core business and expand this internal knowledge by purchasing external knowledge when necessary. As a trading company, you need to know which product groups can offer reliable stability. What and how the customer will consume in the future is therefore crucial. For this reason, we work together with global trend analysis bureaus.«

Buying Director, Retail Industry

ACTION REQUIRED FOR RISK MANAGEMENT

As part of the expert interviews conducted, various fields of action can be identified which combine the current **requirements for improved support** of risk management processes.

For proactive risk management, the need for further development of the supply chain organisation into a more flexible, transparent and thus more resilient supplier network and improved early detection were identified as important fields of action. The evolution of the supply chain organisation **towards a resilient supply chain** in proactive risk management also has a significant impact on risk response and recovery from a disruptive incident. The fields of action of proactive risk management therefore also represent important aspects of reactive risk control. If the basic flexibility and transparency of the supply chain has not been optimised in a focused manner before the risk event, this cannot be achieved in an ad hoc way in the disruptive crisis situation as reaction and recovery is no longer possible.

Exactly this transparency internally and along the supply chain, as well as the flexible reaction possibilities and redundancies of the supply chain are the basis for reactive instruments and measures.

Based on this insight, the fields of action currently identified in business practice of **transparency, flexibility** (including redundancy) and **cooperation** across the various sectors and company sizes can be summarized for both reactive and proactive risk management. These aspects also coincide with the factors identified in the literature for supply chain resilience [3, 11]. In addition, **risk awareness**, i.e. the identification and assessment of possible disruptive risks and the fundamental creation of a risk culture and organisation, is another central aspect of supply chain risk management. These four identified fields of action are described below.

1. Risk Awareness

That disruptive events in global supply chains are inevitable was a point emphasised in all expert interviews. In addition to this fundamental **recognition that disruptive risks cannot be avoided**, the field of action of risk awareness primarily comprises the most complete possible **identification** of potential disruptive risks affecting the supply chain, the structured **development of action plans** and the best possible **early recognition of risks** in order to extend the short warning times.

Figure 3: Fields of action for the risk management of disruptive events

»You can create an awareness in advance where these disruptive risks are. And then, in my opinion, the moment you become aware of it, you need to set up a strategy: how do you deal with this risk? There may be a way to create a safety stock. Or the risk is so big that you definitely need a second source.«

Dr. Stefan Geraedts, Director Logistics, Behr-Hella Thermocontrol GmbH

»Preparing a contingency plan is no longer purely reactive crisis management, but is already part of a proactive approach. That is why I would always favour proactive risk management. This doesn't mean that risks can be completely avoided, but you can at least reduce their impact.«

Prof. Dr. Michael Henke, Director of Fraunhofer Institute for Material Flow and Logistics IML

Assessing the impact of the various possible disruptions **as realistically as possible** is also an important task in this field of action, as these assessments can be used to manage priorities and investments.

»What happens if, for example, logistics locations can no longer be productive overnight due to unforeseen events? We have developed appropriate scenarios and strategies for dealing with these situations.«

Logistics Department Manager, Retail Industry

After an incident has occurred, **the rapid identification of the fault**, its effects on the supplier and customer supply chain and the **definition of the necessary measures** is both important and complicated. Most of the companies surveyed only use an integrated, near-real-time and technology-supported solution to a limited extent or are currently planning a system introduction.

2. Transparency

During the course of the interviews, transparency was identified as an important field of action, particularly with regard to the **company's own information and core data**, the **transfer of information between companies** in a supply chain and the **integration of external environmental information** and developments.

» Transparency is the factor that can make or break whether a risk is dealt with successfully or not. «

Dr. Dirk Dreher, Head of Logistics Planning, BMW Group

As was shown in the specialist interviews, however, this in-depth data transfer with suppliers is particularly complicated to implement in many cases due to different objectives, lack of trust, or different, competing customer relationships.

3. Flexibility

Flexibility describes the ability of a supply chain and the companies involved to **adapt to new circumstances** [11]. Ideally, this flexibility will relate to suppliers, products, customers and internal processes, i.e. it affects the entire supply chain. A central area for achieving flexibility is the **establishment of reliable redundancies**. These redundancies can be implemented in relation to distributed or strategically retained production capacities, different, geographically distributed suppliers of identical parts or safety stocks [15].

During the course of the expert interviews, it became clear that the possibilities of structured planning of resiliencies, especially in sourcing, are strongly influenced by the products purchased and regional conditions. Redundancy in material supply due to high safety stocks is usually not the solution of choice, both for reasons of capital commitment and due to the difficulty of forecasting future product shortages. In many companies, the analysis of these redundancy aspects takes place purely manually, and not in a structured way. Even a centralised view and control of redundancies across the different areas is only slowly being implemented in the companies.

» If all partners in the value chain now suddenly had a flexibility corridor that was twice as large, then dealing with disruptive events would, of course, be much better than if this were not the case. But the problem is that flexibility is appreciated, but not necessarily paid for by the customers. «

Prof. Dr.-Ing. Axel Wagenitz, Hamburg University of Applied Sciences (HAW Hamburg)

4. Cooperation

The **close and as far as possible trusting cooperation** with the partners along the entire value chain represents a further success factor mentioned in the interviews. The ideal picture includes not only cooperation with the direct supplier and the direct customer, but also **cooperation with tier-n suppliers** and downstream customer entities. This cooperation along the entire supply chain, in particular, has to be focused on as a factor that will become increasingly important in the future. In relation to the matter of transparency, the **questions of trust, autonomy and data sovereignty** must be considered and addressed. On the subject of cooperation, the issue of preventing the loss of value-added partners through financial shortages in crisis situations continues to be an increasingly important consideration.

In summary, it can be seen, especially in IT support, that even internationally operating companies in failure-prone industries often react to disruptive events without specific software tools and structures and switch to existing **manual and non-standard tools**. Communication with suppliers and customers also often takes place without system support and, in the event of a fault, without uniform standards. Both interviews and recent studies [2] have shown that if IT support is available at all, a great deal of it is only in the form of generally available spreadsheet tools. Reasons for this reluctance to invest in software-supported risk management include **budget restrictions, an outdated IT infrastructure, lack of personnel, fear of cyber attacks and regulatory reasons**. Establishing this fundamental readiness for system- and technology-supported risk management of disruptions is an internal company task that must be dealt with initially in order to realise further potential.

NEW TECHNOLOGIES AND METHODS

Current technological developments enable improved or new possibilities in risk management. These fundamental trends and technologies can enable the development of tools, specific measures and structures that further develop basic resilience and specific risk responses.

CURRENT TRENDS AND DEVELOPMENTS IN SUPPLY CHAIN MANAGEMENT

As shown in figure 4, supply chains are affected by various **environmental developments as well as market and social trends**. Based on these external trends and market developments, together with the increase in disruptive events, risk management must **also adapt to the constantly changing circumstances in the future** [10, 16, 17].

In response to these external demands on companies and supply chains, various internal trends can be identified that respond to these changes. These endogenous developments [10] focus on the following areas:

- Digitalisation of business processes
- Business analytics
- Transparency in the value-added chain
- Networking/cooperation
- Automation
- Decentralisation

Both the results of the expert interviews and previous studies show that small and medium-sized enterprises in particular are only just beginning to fully recognise the potential of digitalisation, including for risk management, and to derive actions from this. The larger and more international a company is structured, the more aspects of data transparency and digital networking and support are already implemented.

TECHNOLOGIES FOR DEALING WITH FUTURE DISRUPTIVE EVENTS

The trends described above place increased demands on risk management, but at the same time open up **potential to meet the identified needs for action**, especially through endogenous developments together with new technologies. The relevant technologies, some of which are already available, are described below.

Big Data and Artificial Intelligence

The combination of different, constantly growing data sources creates a large new and processable data collection, which is called big data [19]. This data collection enables new possibilities for the **analysis of cause-effect relationships, the prognosis of scenarios** and **support in decision-making.**

Figure 4: Presentation of current supply chain development trends [7, 10, 18]

As such, data analyses can no longer only uncover systematics in the past (descriptive) and identify causal relationships, but can also extend them into the future within the framework of predictive analysis, provided the data contains these structures. In a further step, it is even possible to analyse and evaluate various possible alternatives, so that recommendations for action can be generated and evaluated against each other during the course of the prescriptive analysis.

The combination of self-learning components of artificial intelligence (AI) with expert knowledge and big data results in a decision support and forecasting capability that can **recognize patterns in complex environmental situations**. These patterns would either have remained hidden to humans due to their dynamics and complexity or could only be extracted with a large degree of manual effort. Increasing supply chain transparency through novel analysis capabilities also has a positive impact on proactive risk identification and risk control [16]. [19]

Simulation

The availability of larger data volumes, faster computing times and the integration of simulation into systems and processes continues to open up new potential on the basis of simulation applications. Essentially, simulation describes the **depiction of a reality in executable simulation models,** which, with regard to the aspects to be examined, behave as closely as possible to reality. By carrying out simulation experiments, in which **statements about the system behaviour** (mostly over time) are derived under different settings and parameters, the influences and the basic system behaviour are investigated.

Only by the subsequent transfer of the simulation results to the actual, mostly very dynamic and complex application cases, conclusions and measures can be derived which could not be obtained analytically due to the high dynamics and the complexity of reality. The simulative assessment of different risk situations as well as different risk reactions leads to a **better understanding of the effects of disruptive events** and more justified and accurate proactive preparations [16]. [22]

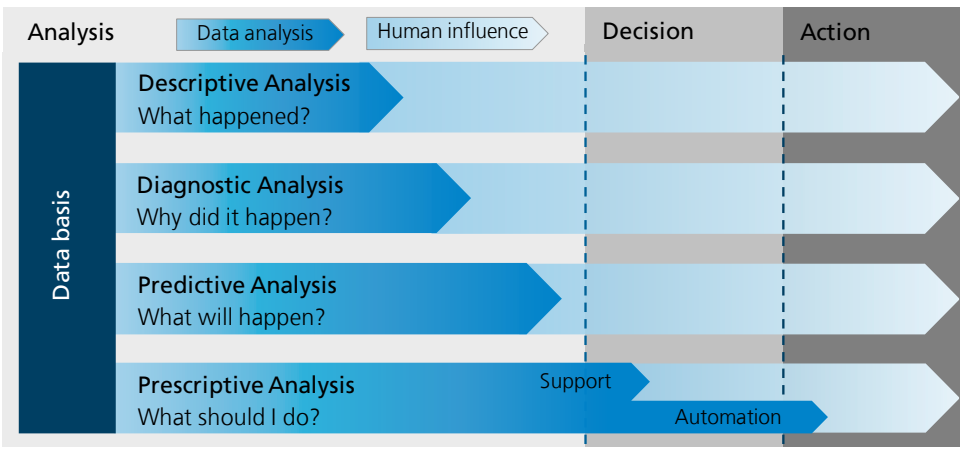

Figure 5: Possibilities of data analysis (adapted from [20, 21])

Blockchain and Smart Contracts

Blockchain technology provides a way to organise data exchange, transactions and contracts in a network in a **decentralised manner and without intermediaries controlling** the system. The distributed checking and storage of information by all parties involved using the distributed ledger, i.e. a distributed logbook, and the coded reference to the previous stored block prevents manipulation and provides redundant, secure data storage (**irreversibility**). Only if all involved nodes of the network confirm the accuracy of the resulting block chain and the reference of new transactions (**consensus mechanism**), new information is stored. Error-free entries can be easily repaired and checked with redundant data storage. By integrating conditions and causal consequences, it is also possible to integrate intelligent, automatically executing contracts, known as **smart contracts,** which enable the automation of interactions. As such, this technology can be used to streamline processes, establish trust and track transactions with absolute certainty. [23]

» With blockchain, we now have the option of creating the necessary transparency throughout value-added networks. As a result, you can implement risk management far better than you could previously. «

Prof. Dr. Michael Henke, Director of Fraunhofer Institute for Material Flow and Logistics IML

METHODS AND SOLUTIONS FOR DEALING WITH DISRUPTIVE EVENTS

The future developments and applications primarily considered by the experts and decision-makers together with the IT solutions and methods currently under discussion are described below on the basis of the following fields of action: **risk awareness, transparency, flexibility and cooperation**. The introduction and use of modern tools by a suitably qualified and structured risk management team or respective risk officer is fundamental to their successful use.

» Without good people involved in a good process, I don't think that a solution or a software will help to bring a company to a very high level of risk management. Before implementing a tool, the team itself becomes very important «

Andrea Scammacca, International Consultant

1. Risk Awareness

Risk awareness focuses, among other things, on the **risk culture** underlying the subsequent management of disruptive events in the supply chain. This risk culture is not developed through technical solutions, but through a general engagement with vulnerability and the **essential risk analysis**, which should also be promoted by top management. Tools can continue to be used to support the identification of potential risks, structured **process standardisation** and the consideration of all influencing factors. Particularly in large, transnational companies, risk information and responses are often observed and collected at a central location across all business units and companies so as to achieve a **risk picture that is as complete as possible** and a **company-wide coordinated risk strategy.**

This collection and evaluation of information is only possible with **modern software solutions.** In particular, extending this central data basis to the entire supply chain requires digital systems and solutions that can meet the challenges described under the field of transparency.

» We effectively have a general overview and exchange of information across all our national affiliates. It is then concentrated and fed back into the individual foreign subsidiaries in terms of coordinating appropriate strategies and measures, and implementing these measures.«

Logistics Department Manager, Retail Industry

Specialist experts and decision-makers see more direct potential in the **rapid identification of risks and near-real-time analysis of their effects.** By extending advance warning times - which is only partially possible - but above all by quickly identifying events that have occurred and their direct and indirect effects on the supply chain, responses can be initiated more quickly or communication with customers and suppliers can be intensified in a targeted manner. **Monitoring platforms** such as DHL Resilience360, Risk Radar of RiskMethods GmbH, resilinc or A1 Tracker are examples that support data analysis and data visualisation as well as the identification of risks or their effects. The visualisation of processes and their distribution is also a great advantage for creating a well-founded threat situation. The **centralisation of information and risk management** plays a particularly important role here, to be able to react to possible risks in a coordinated manner, at least within a company. This central data basis can also be made possible by comprehensive system support.

The comparatively very low probability of a disruption occurring can - if at all possible - only be determined approximately from historical data and patterns [7, 15]. To take this adequately into account, despite this low probability, methods of big data analytics and AI algorithms can be used in systems that are optimised for this purpose so as to recognise trends or **correlations in unstructured mass data** and to forecast them into the future. In this way, **measures can be prioritised or investments evaluated** in order to adapt the resilience of the supply chain to the risk profile. The automated, AI-based evaluation of freely accessible information on the Internet using what are known as crawlers allows a large number of different, often unstructured sources (e.g. Twitter) to be analysed and events to be detected early.

» For the first time, the internet is offering the possibility of recognising disruptive events occurring elsewhere in the world very quickly, and then evaluating this information using digital methods. With the appropriate crawlers, a wide variety of different sources of information can be monitored. «

Dr. Michael Müller-Bungart, Senior Manager, Deloitte Consulting GmbH

2. Transparency

The **transparency within a company** affects master data, supply chain structures and the current risk situation in equal measure. **Geographical supplier clusters,** for example, can only be identified and potential consequences can only be analysed through well maintained and structured information. Here, system-supported and standardised processes can be used to **create reliable data bases** for analyses and modern evaluation technologies such as artificial intelligence.

A coordinated and well developed **IT infrastructure** is the basis for a uniform, non-redundant data management and, consequently, up-to-date and reliabie results. The foundation of the IT infrastructure for risk management is usually an ERP system or a comparable platform, which provides the operational database and can be extended by connected systems and tools [24]. **Real-time tracking of material flows** is also possible through modern technologies such as RFID, the Internet of Things and 5G.

The **tier-n transparency**, i.e. transparency along the various companies in the supply chain, can achieve various degrees of implementation, ranging from knowledge of the structure and organisation of supplier relationships and product origins to **reliable information and planning transparency**. The relevant information in the context of n-tier-transparency goes beyond the data classically contained in ERP systems, as it also includes, for example, the suppliers' suppliers or the customers' customers in order to present **a picture of a supply chain that is as complete as possible**. Modern and novel solutions that optimise this transparency within supply chains must at the same time offer a high degree of confidence in the use and accessibility of shared information [9]. Since independent companies in a supply chain continue to act opportunistically and in some cases are also in direct competition, data sovereignty plays a major role here.

One way of **ensuring data sovereignty** while at the same time maintaining transparency of the necessary information is, for example, the provision of data linked to a specific purpose of use within the framework of the International Data Spaces Association [25] or the **tamper-proof documentation** of the information exchange using block chain technology.

» There is often simply no foundation of trust when it comes to passing on information. There are, however, new possibilities to establish this trust, especially through blockchain technology. «

Prof. Dr.-Ing. Axel Wagenitz, Hamburg University of Applied Sciences *(HAW Hamburg)*

3. Flexibility and Resilience

High flexibility, especially through **strategically positioned redundancies**, is what makes risk reactions possible in the first place. In particular, when setting up these redundancies in the form of stocks, alternative suppliers or extended production or storage capacities that are normally unused, the **balance between investments and the benefits generated** must be considered. Flexibility in the undisturbed environment generates higher costs than a lean supply chain avoiding all forms of waste. The effectiveness of individual redundancies can be analysed, among other things, by **simulating various scenarios** to illustrate a cost-benefit analysis with regard to the measures and the associated improvement in resilience. **Simulation tools** such as AnyLogic, OTD-NET, Plant Simulation or Supply Chain Guru can be used for the simulation of entire supply chains.

4. Cooperation

The cooperative collaboration between the companies in a supply chain underlies all the previously mentioned fields of action of optimised supply chain risk management. In addition to the more extensive **networking of planning and communication processes**, financial cooperation, i.e. ensuring the survival of all supply chain partners in disruptive crises, is also an important part of cooperation.

Therefore, cooperation concerns the **information, material and financial flows** of a supply chain. The joint response in the event of an incident enables both the effectiveness and, especially in the case of proactive preparation and planning, the best possible cost-effectiveness of emergency measures that can otherwise be very expensive [7]. Through cross-company coordination and implementation of **business continuity plans**, standard reactions to restrictions in functionality can be defined, thus enabling a uniform risk reaction. Collaborative demand planning or joint production planning are also applications of collaboration. Above all, cross-company demand and capacity management in conjunction with inventory transparency allows for numerous possibilities within the framework of a coordinated and optimal risk reaction under the existing restrictions. This collaborative cooperation in the supply chain has been requested and planned (in theory) for a long time, implementation in business practice does not take place as standard due to **challenges both in trust and autonomy.**

ASSESSING THE AVAILABILITY OF SOLUTIONS AND TECHNOLOGIES AND THE CURRENT ACTIONS REQUIRED

As a result of technological advances, new technologies such as **artificial intelligence** and **blockchain** are ready for use in business practice or are close to being suitable for use. However, **management processes and infrastructures** are not yet geared to these new technological possibilities. Adapting organisational and management processes and structures to these new technologies is one of the major challenges. The technology of simulation has already existed for a long time, but the combination with self-learning and intelligent systems of AI opens up **new application possibilities.** In particular, the selection of meaningful scenarios and the evaluation of the simulation results have been associated with great effort in the past. In the future, coordinated processes and new links will make it possible to realise greater potential with less work from personnel in order to assess risks with regard to their effects and interactions and to check the **suitability of various proactive and reactive measures.**

As part of the risk infrastructure in companies, analysis and visualisation platforms already enable uniform processes, cross-company data bases and the structured integration of external information through various options. However, solutions of this type are not yet widely deployed or integrated along the supply chain. With the use of this IT solution in particular, employees are only able to **analyse and evaluate complex risk situations as proactively as possible** through professional training.

Technological possibilities already exist for the use of information and coordination platforms for the entire supply chain in order to create transparency while respecting data sovereignty and autonomy, to plan measures proactively and to implement them in a coordinated manner in the event of a fault. At a cross-company level, the profitable and effective use of these tools requires **companies to be willing** to adopt these new possibilities and for **processes to be aligned**.

CONCLUSION AND OUTLOOK

The significance of disruptive events for supply chains will continue to increase in the future. The primary risks under focus are shifting towards cyber attacks, increased and sometimes more serious natural catastrophes, major IT-related disruptions and acts of terrorism [2]. In terms of risk management, these changing and increasing disruptive risks are countered by **new technologies, methods and specific solutions** that support and optimise either the forecasting and early detection, the fundamental increase and monitoring of the **resilience of a supply chain,** or the reactive measures in the response and recovery phases. On the one hand, the digital transformation of value creation systems opens up new potential for **system-supported risk management** and more strongly networked added value; on the other hand, however, it also results in change and new risks to the supply chain though cyber risks and dependencies on IT systems [9], which in turn must be dealt with.

In the expert interviews conducted, the fields of action of risk awareness, transparency, flexibility and cooperation in the supply chain were identified. The field of risk awareness in particular combines organisational and personnel methods and structures with technological solutions for risk identification and early detection. Within these fields of action, both modern technologies such as artificial intelligence, big data analysis and simulation and the IT solutions based on them as well as general methods and structures can enable and achieve new potentials. While many companies have a good command of reactive measures following a disruptive incident and are developing them further, there is still potential for optimisation in proactive management, i.e. developing resilience and early detection of disruptions. These are mainly due to the probabilities of occurrence that are difficult or even impossible to predict, the complicated analysis of the effects on complete supply chains across all levels and the large number of potential reaction measures and their suitability assessment. Due to the **increasing influence of disruptive events**, which also have an overall direct impact on all parts of the supply chain, the **recognition of the need** for a systematic and technology-based proactive management of these uncertainties and thus the **willingness to invest** is constantly increasing. Thanks to current technological developments, this „real" supply chain risk management, respecting both data sovereignty and overall optimality at the same time, will also be achieved in practice in the future for the first time. Further trends and current research approaches, such as decentralisation and artificial intelligence in the context of the Internet of Things, will open up **new possibilities and potentials for risk management** in the future.

» At some point in the future, objects in the Internet of Things will be able to go online worldwide and obtain information about the respective risk exposure on board. In this cyber-physical environment, intelligent objects will then be able to carry out risk assessments in real time and, depending on the results, place themselves along the route of the material flow independently.«

Prof. Dr. Michael Henke, Director of Fraunhofer Institute for Material Flow and Logistics IML

REFERENCES

[1] Christopher, M. u. Holweg, M.: Supply chain 2.0 revisited: a framework for managing volatility-induced risk in the supply chain. International Journal of Physical Distribution & Logistics Management 47 (2017) 1, pp. 2–17

[2] Supply Chain Resilience Report 2019, Business Continuity Institute, Caversham, Berkshire, UK 2019

[3] Biedermann, L.: Supply Chain Resilienz. Wiesbaden: Springer Fachmedien 2018

[4] ten Hompel, M. u. Henke, M.: Logistik 4.0 – Ein Ausblick auf die Planung und das Management der zukünftigen Logistik vor dem Hintergrund der vierten industriellen Revolution. In: ten Hompel, M., Vogel-Heuser, B. u. Bauernhansl, T. (Hrsg.): Handbuch Industrie 4.0. Berlin: Springer Vieweg 2017, pp. 247–268

[5] Romeike, F. u. Huth, M.: Struktur des Risikomanagements in der Logistik. In: Huth, M. (Hrsg.): Risikomanagement in der Logistik. Springer Fachmedien Wiesbaden 2016, pp. 49–84

[6] DIN ISO 31000:2018-10, Risikomanagement - Leitlinien (ISO 31000:2018)

[7] Huth, M. u. Romeike, F.: Grundlagen des Risikomanagements in der Logistik. In: Huth, M. (Hrsg.): Risikomanagement in der Logistik. Springer Fachmedien Wiesbaden 2016, pp. 13–47

[8] Norrman, A. u. Lindroth, R.: Categorization of Supply Chain Risk and Risk Management. In: Brindley, C. (Hrsg.): Supply Chain Risk. Abingdon, Oxon: Taylor and Francis 2004, pp. 14–27

[9] Kersten, W., Schröder, M. u. Indorf, M.: Potenziale der Digitalisierung für das Supply Chain Risikomanagement: Eine empirische Analyse. In: Seiter, M., Grünert, L. u. Berlin, S. (Hrsg.): Betriebswirtschaftliche Aspekte von Industrie 4.0. Wiesbaden: Springer Fachmedien Wiesbaden 2017, pp. 47–74

[10] Kersten, W.; Seiter, M.; von See, B-; Kackius, N.; Maurer, T.: Trends und Strategien in Logistik und Supply Chain Management. Chancen der digitalen Transformation. Bundesvereinigung Logistik (BVL), Bremen 2017

[11] Zitzmann, I.: Supply Chain-Flexibilität zur Bewältigung von Unsicherheiten. Taktisch-operative Potenzialplanung zur Schaffung von Robustheit, Resilienz und Agilität. Bamberg: University of Bamberg Press 2018

[12] Schlegel, G. L. u. Trenz, R. L.: Risk Management: Welcome to the new normal. Supply Chain Management Review (2012) (Jan/Feb)

[13] Christopher, M. u. Peck, H.: Building the Resilient Supply Chain. The International Journal of Logistics Management 15 (2004) 2, pp. 1–13

[14] Hohenstein, N.-O., Feisel, E., Hartmann, E. u. Giunipero, L.: Research on the phenomenon of supply chain resilience. International Journal of Physical Distribution & Logistics Management 45 (2015) 1/2, pp. 90–117

[15] Sheffi, Y. u. Rice, J. B.: A Supply Chain View of the Resilient Enterprise. MIT Sloan Management Review 47 (2005) 1

[16] Schrauf, S.; Geissbauer, R.; Schneider, J.; Hermans, M.: Connected and autonomous supply chain ecosystems 2025, PwC, 2020

[17] Münchener Rückversicherungs-Gesellschaft: NatCatSER VICE. Natural catastrophe know-how for risk management and research, 2020. https://natcatservice.munichre.com/

[18] Annual Risk Report 2020, Resilience360 GmbH, Troisdorf / Spich2020

[19] Bitkom e.V.; DFKI: Entscheidungsunterstützung mit Künstlicher Intelligenz. Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung. 2017

[20] Bedeutung von Daten im Zeitalter der Digitalisierung, Möller, F., Spiekermann, M., Burmann, A. u. Pettenpohl, H., 2017

[21] Hagerty, J.: 2017 Planning Guide for Data and Analytics, 2016. https://www.gartner.com/en/documents/3471553/2017-planning-guide-for-data-and-analytics

[22] Gutenschwager, K., Rabe, M., Spieckermann, S. u. Wenzel, S.: Simulation in Produktion und Logistik. Berlin, Heidelberg: Springer Berlin Heidelberg 2017

[23] Blockchain und Smar Contracts: Effiziente und sichere Wertschöpfungsnetzwerke, Jakob, S., Schulte, A. T., Sparer, D., Koller, R. u. Henke, M., Dortmund 2018

[24] All together now. Third party governance and risk management, Extended enterprise risk management global survey 2019, Park, K., Griffiths, D., Bethell, M. u. Sen, S., 2019

[25] International Data Spaces e. V.: Industrial Data Spaces. The Principles, 2020. https://www.internationaldataspaces.org/the-principles/