

Lech Bukowski

Reliable, Secure and Resilient Logistics Networks

Delivering Products in a Risky
Environment

 Springer

Reliable, Secure and Resilient Logistics Networks

Lech Bukowski

Reliable, Secure and Resilient Logistics Networks

Delivering Products in a Risky Environment

Lech Bukowski
WSB University
Kraków, Poland

ISBN 978-3-030-00849-9 ISBN 978-3-030-00850-5 (eBook)
<https://doi.org/10.1007/978-3-030-00850-5>

Library of Congress Control Number: 2018958495

© Springer Nature Switzerland AG 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*This book is dedicated to my wife Ewa
with thanks for over 50 years of good life
together.*

Preface

Contemporary business activity, both real (including industrial and agricultural production, services and trade) as well as virtual (i.e. capital and banking activity, investment funds and financial markets) is developing particularly fast on a global scale. This entails, among others, a continuous increase in the complexity of systems within which integrated business, production and service processes are implemented, as well as the need to make key decisions based on imperfect knowledge resulting from the uncertainty, incompleteness and ambiguity of available data and information, and limited rationality of inference.

Such complex systems are also modern logistic networks which 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. Logistics as the field of knowledge is defined differently in the European zone (e.g. the definition of The European Logistics Association) and in the American zone (e.g. the definition of The Council of Supply Chain Management Professionals). In this work, logistics is understood as a transdisciplinary field of scientific 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.

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. Hence, the concept of Total Logistic Management, developing by the author of this work since 1996 as the core idea of annual conferences under the same name. The concept was based on the following assumptions:

- (a) The complexity of logistics systems and the emergent nature of their properties. Modern supply chains are complex engineered system of systems (usually with a network structure) whose properties, due to multiple interdependency relations between their constituent elements and the environment, are of emergent character, therefore it is not possible to determine them solely on the basis of inherent properties of constituent elements.
- (b) Multifaceted issues. A comprehensive approach to logistics systems requires consideration of three basic aspects, namely:
 - The spatial extension of the logistics infrastructure and its surroundings, where the boundary between the system and its surroundings is usually vague or fuzzy;
 - Temporary continuity and variability of logistics processes in terms of the so-called 'Life cycle' and sustainability;
 - A holistic approach from a technical, economic and socio-ethical perspective.
- (c) Imperfection of available knowledge and decision-makers. Knowledge, on the basis of which decisions are made, is based in many cases on uncertain, incomplete and ambiguous data and information, therefore it is imperfect. Furthermore, decision-makers are guided in practice by the principle of limited (or bounded) rationality which means a large impact of the subjective assessment of both the current situation and the utility value of the decision taken.
- (d) The importance of the role of risk in making decisions. Modern logistics networks should be designed and implemented in order to provide them with the highest possible level of reliability, security, safety and resilience. However, 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 aim of this work is to synthesise 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 dependable product delivery assurance. In order to quantitatively assess dependability, the service continuity oriented approach has been applied. This approach is based on the methodology of service engineering and is closely related to the idea of resilient enterprise as well as to the concept of disruption-tolerant operation. On this basis a framework for evaluation of logistic networks operational risk and dependability has been developed and its applicability shown in several practical examples.

The content of the book has been divided into six main parts. In the first of them—Introduction—an analysis of the logistic concepts development was made. On this basis, a system of concepts and definitions on which modern logistics is based has been proposed. In Chap. 2 the concept of imperfect knowledge was presented as the foundation for further considerations. Assessment knowledge about engineered systems is based on imperfect data and information obtained within the imperfect

knowledge chain. Therefore, the process of knowledge creating and managing must take into account uncertainty modelling methods. The measure of excellence of acquired knowledge is knowledge maturity level which forms the foundation for imperfect knowledge based concept of risk. The proposed operational risk model is based on these assumptions.

Chapter 3 was devoted to the description of engineered systems based on imperfect knowledge. A full description of the assessed system will be carried out both in terms of system and process approach using both topology- and flow-based methodology. The infrastructure description pays particular attention to its complexity and dependencies between elements of the structure, especially in the case of global supply networks. Instead, the process approach is based on the service engineering principles to describe the specificity of the delivery processes (supply, demand and distribution) as accurately as possible. A quantitative description of the system will contain both performance and operability related measures.

Designing complex engineered system for the risky environment is a comprehensive process including two main steps, namely creating reliable system's infrastructure and assurance process continuity. In case of logistics networks architecting reliable engineered system of systems is based on the principle of High Reliability Organisations, whereas the process continuity ensuring is established on the concept of Resilient Enterprise. Detailed describing of the system designing process can be found in Chap. 4.

Modelling and simulation of logistics networks is divided into four main stages: modelling of logistic infrastructures using an agent based approach, modelling of logistic processes applying a dynamic based approach, modelling of demand variation using a probabilistic approach, and modelling of disturbances with an event driven approach. All these processes are described in Chap. 5.

Chapter 6 is a summary of previous chapters and serves as their practical illustration. A general framework for Evaluation of Logistic Networks Operational Risk and Dependability—ELNORD has been proposed, and three different examples of its application presented. First example concerns a modified PFMEA method (Process Failure Mode and Effects Analysis) as representative of a risk-oriented static approach. Next example is an expert system with fuzzy reasoning based on a process-continuity oriented approach. The last one uses a vulnerability related dynamic approach to create an expert system with agent-based simulation.

The end of the book constitute: conclusions and concluding considerations and terminology of the most important terms used in the book (Appendix).

Acknowledgements

This publication has been accomplished as a part of a research project funded by Prof. Henryk Walica Scientific Scholarship Fund. Therefore, I would like to express my gratitude to the WSB University in Dabrowa Górnicza for supporting my research. In addition, my thanks belong to Judyta Rak for significant help in polishing my English.

Contents

1	Introduction	1
1.1	A Brief History of Logistics Development	1
1.2	Defining the Key Terms in Logistics	4
	References	6
2	Assessment Knowledge About Engineered Systems	9
2.1	Concept of Imperfect Knowledge	9
2.1.1	From Knowledge Pyramid to Imperfect Knowledge Chain	9
2.1.2	Data and Information Imperfection	12
2.1.3	The Process of Knowledge Creating and Managing	17
2.1.4	Knowledge Maturity Assessment	21
2.2	Uncertainty Modelling	23
2.2.1	General Concept of Uncertainty	23
2.2.2	Uncertainty Modelling Methods	29
2.3	Imperfect Knowledge Based Concept of Risk	35
2.3.1	Defining Risk	35
2.3.2	The Role of Background Knowledge in Risk Analysis	37
2.3.3	Risk Types and Its Metrics	41
2.3.4	Modelling Operational Risk Based on the Imperfect Knowledge Concept	54
	References	57
3	Describing Engineered Systems	59
3.1	Infrastructures—Topology-Based Methodology	59
3.1.1	System Approach—Systems Engineering	59
3.1.2	Complexity and Emergence—System of Systems and Network Organisation	67

3.2	Processes—Flow-Based Methodology	74
3.2.1	Process Approach—Service Engineering	74
3.2.2	Delivery Processes—Supply, Demand and Distribution . . .	79
3.3	Attributes of Engineered Systems	85
3.3.1	Performance-Related Measures	85
3.3.2	Operationality Related Measures	88
	References	91
4	Designing Complex Engineered Systems for the Risky Environment	93
4.1	Creating Reliable Infrastructures	93
4.1.1	System of Systems Engineering	93
4.1.2	Engineered System of Systems and Its Main Attributes . . .	95
4.1.3	Architecting Reliable ESoS	98
4.1.4	Building High Reliability Organisations	104
4.2	Assurance Process Continuity	110
4.2.1	From High Reliable Organisation Concept to Resilience Engineering Approach	110
4.2.2	Resilience Science—Transdisciplinary Perspective	112
4.2.3	Organisational Resilience—The Concept of Resilient Enterprise	120
4.2.4	From Resilient Enterprise Concept to Process Continuity Ensuring	124
4.3	Managing Operational Risk—The Concept of Dependable Operating	129
4.3.1	From Reliability Engineering to Dependability Engineering	129
4.3.2	Disruption-Tolerant Operating—The Continuity Oriented Approach	134
4.3.3	Operational Risk Based Concept of Dependability	137
	References	140
5	Modelling and Simulation of Logistic Networks	151
5.1	Modelling and Simulation of Complex Engineered Systems	151
5.1.1	Main Principles of Modelling and Simulation	151
5.1.2	The Life Cycle of a Modelling and Simulation Process . . .	159
5.2	Modelling of Logistic Infrastructures—Agent Based Approach . . .	164
5.2.1	Fundamentals of Agent-Based Modelling and Simulation	164
5.2.2	Using Agent-Based Modelling and Simulation in Logistics	168
5.3	Modelling of Logistic Processes—Dynamic Based Approach	171
5.3.1	General Rules for Managing the Flow Processes	171
5.3.2	Classification of Processes and Their Properties—APQC Model	173

5.3.3	Process Specification Standards	174
5.3.4	Process Dynamic Modelling and Simulation	185
5.4	Modelling of Demand Variation in Logistic Networks—Probabilistic Approach	189
5.4.1	Predictable Volatility	189
5.4.2	Unpredictable Variability	193
5.5	Modelling of Disturbances in Logistic Network—Event Driven Approach	197
5.5.1	Identification of Sources of Risk, Threats and Hazards.	197
5.5.2	Modelling of Exposures in Logistics Networks	200
	References	210
6	Assessment Operational Risk and Dependability of Logistic Networks—Application Examples	215
6.1	A Framework for Evaluation of Logistic Networks Operational Risk and Dependability—ELNORD.	215
6.2	Application Examples of the ELNORD Framework	221
6.2.1	A Risk Oriented Static Approach—A Modified PFMEA Method	221
6.2.2	A Process Continuity Oriented Approach—An Expert System with Fuzzy Reasoning for Disruption Risk Prediction in Logistics Networks	234
6.2.3	A Vulnerability Related Dynamic Approach—An Expert System with Agent-Based Simulation	240
	References	250
	Conclusions and Concluding Considerations.	255
	Appendix: Terminology	259

Abbreviations

ABM	Agent-Based Modelling
ABS	Agent-Based Simulation
AIR	Average Individual Risk
ANN	Artificial Neural Networks
APQC	American Productivity and Quality Center
ARIS	Architecture of Integrated Information System
BCM	Business Continuity Management
BPMN	Business Process Model and Notation
CBR	Case-Based Reasoning
CCA	Cause and Consequences Analysis
CDF	Cumulative Distribution Function
CHL	Check List Analysis
CIP	Continuous Improvement Process
CIT	Communication and Information Theory
CST	Classical Sets Theory
DDSC	Demand Driven Supply Chain
DES	Discrete Event Simulation
DFD	Data Flow Diagram
DTN	Disruption-Tolerant Network
DVV	Data Veracity Value
ELNORD	Evaluation of Logistic Networks Operational Risk and Dependability
EPC	Event-driven Process Chain
ERD	Entity Relationship Diagram
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
ESoS	Engineered System of Systems
ETA	Event Tree Analysis
FAR	Fatal Accident Rate
FMEA	Failure Mode and Effects Analysis

FMECA	Failure Mode, Effects and Criticality Analysis
FRAM	Functional Resonance Analysis Method
FTA	Fault Tree Analysis
GIS	Geographic Information System
GIT	Generalized Information Theory
GTU	Generalized Theory of Uncertainty
HAZOP	Hazard and Operability Studies
HRA	Human Reliability Assessment
HRO	High Reliability Organization
ICT	Information and Communication Technologies
IK	Imperfect Knowledge
ITS	Intelligent Transportation Systems
IUV	Information Utility Value
JIT	Just in Time
KML	Knowledge Maturity Level
KPQ	Knowledge Processing Quality
LN	Logistic Network
LP	Logistics Process
LS	Logistics System
LSLIRE	Large Scale, Large Impact, Rare Event
LSS	Large-Scale Systems
M&S	Modelling and Simulation
MAS	Multi-Agent Systems
MTBF	Mean Time Between Failures
MTTFF	Mean Time To First Failure
NFST	Nonstandard Fuzzy Sets Theory
PDF	Probability Distribution Function
PFMEA	Process Failure Mode and Effects Analysis
PHA	Preliminary Hazard Analysis
PLL	Potential Loss of Life
PSA	Process Safety Analysis
RE	Resilience Engineering
ROI	Return on Investment
RP	Random Process
RPN	Risk Priority Number
RSC	Resilient Supply Chain
RTE	Real-Time Enterprise
SC	Supply Chain
SCM	Supply Chain Management
SCOR	Supply Chain Operations Reference
SCRM	Supply Chain Risk Management
SCS	Supply Chain Sustainability
SDM	System Dynamic Modelling
SE	Systems Engineering
SFST	Standard Fuzzy Sets Theory

SOA	Software Oriented Architecture
SOC	Self-Organized Criticality
SoS	System of Systems
SoSE	System of Systems Engineering
SPC	Statistical Process Control
TAR	Throughput Accounting Ratio
TLM	Total Logistic Management
UST	Unified Service Theory
VaR	Value at Risk
VSM	Value Stream Mapping

Chapter 1

Introduction



1.1 A Brief History of Logistics Development

The authors of most logistic handbooks believe that the modern concept of ‘logistics’ was shaped in the military field as early as the first half of the nineteenth century and included transport, accommodation and supply of military units, as well as transport, storage and supervision of goods intended for the army. In the 1950s, the US started the process of transferring the concept of logistics and related practical experience from the sphere of national defence to business practice. The term ‘business logistics’ was created, which included transport, warehousing and transshipment processes of goods within one enterprise and between different enterprises (e.g. Schönsleben 1998; Stock and Lambert 2001; Shapiro 2001).

It is widely believed (e.g. Lasch 2014) that the turning point in the development of modern logistics was the publication of the article “Note on the Formulation of the Theory of Logistics” (Morgenstern 1955). This publication was an impulse for broader interest in logistics in the civilian area in the USA and around 10 years later in Europe as well. In the German-speaking area, the year 1973 is regarded as the date of the birth of civil logistics, in which the book titled “Business logistics—systems, decisions, methods” (Kirsch et al. 1973) was published. The authors of this book understood logistics as “... shaping, controlling, regulating and implementing energy, information and people flows, in particular materials and products, within a given system and between systems”. Since then, the interest in practical aspects of logistics has grown significantly in Europe, which was reflected in the creation of a pragmatic definition of logistics in the form of the so-called 7R rules (from the English word ‘right’ or from the German ‘richtig’). The interpretation of this rule boils down to stating that the basic task of logistics is to provide the right goods, in the right quantity, at the right time, to the right place, with the right quality, at the right costs along with the right information (Lasch 2014).

At the end of the 1980s, the prominent representative of the German logistic school R. Jünemann generalizes this definition, proposing to understand logistics

as “... a scientific field of knowledge including planning, control and checking of material, energy and information flows within systems” (Jünemann 1989). Such an understanding of the concept of logistics has opened new perspectives for scientists dealing with logistic issues, creating opportunities for searching for theoretical generalizations in the broadly understood area of logistics knowledge. Attempts to distinguish logistics as a field of scientific knowledge having its own theoretical foundation have been undertaken for several years in both Europe and North America. This is evidenced by such works as, for example Albjoren and Haldorson (2002), Mangan et al. (2004), Mentzer et al. (2004), Kovacs and Spens (2007), Shook et al. (2009), Wieland et al. (2016), Stank et al. (2017).

The individual phases and directions of civil logistics development since its foundation to the current state have been described and analysed in detail by many authors (e.g. Lasch 2014; Bukowski 2017). On this basis, the development of logistics in business practice can be divided into six stages, whose brief characteristics are presented in Table 1.1. Stage I covered the sixties and seventies of the twentieth century and was characterized by marketing orientation. The main task of logistics was to provide raw materials, semi-finished products and finished products in accordance with the principle of 7R. The dominant approach at this stage of logistics development was functionally targeted, which means that the optimization of logistic operations was carried out as a part of individual functions (partial optimization) and not as a part of the whole delivery process. This orientation often resulted in problems at the interface of individual functional areas (e.g. bottlenecks in flows and weak links in systems) and prohibited the comprehensive optimization of logistics processes.

In the eighties, a new concept was introduced that emphasized the coordinating role of logistics in managing the flows of all goods between the place of their origin (e.g. by a producer) and the destination (e.g. by a recipient). It was related with an

Table 1.1 The development steps of logistics in business practice

Stage	The main characteristic	The dominant approach	The main goal
I	Delivery of material goods in 3 steps ‘transport—transshipment—storage’	Functional	Effectiveness
II	Coordination of the goods flow within a single enterprise	Regulatory, reactive	Lean
III	Management of goods flow processes within a single enterprise	Systemic, active	Flexibility
IV	Comprehensive management of the goods flow in supply chains	Integration, across the borders of the organization	Agility
V	Optimization of value creation chains within logistic systems	Dynamic, global perspective	Efficiency, leagility and resilience
VI	Virtualization of logistics networks within the 3rd IT platform (SMAC)	Real-time operation (RTE)	Efficiency, leagility and resilience

increase in the complexity of logistics systems and the dynamic development of the new role of logistics, which was the organization of returns of used materials, goods and packaging (so-called reverse logistics). The functional approach gradually gave way to a regulatory approach, in which management decisions were usually reactions to changes taking place over time. The function of the logistic objective was subordinated to the so-called philosophy of ‘lean thinking’, which has mastered both the manufacturing areas (lean manufacturing), as well as organizational and management (lean structures and lean management).

The third phase of the civil logistics development, at the turn of the 1980s and 1990s, was largely a response to significant market changes, namely limiting mass production, allowing full use of economies of scale for flexible adaptation to the needs of the ‘capricious’ customer (economy of scope). Such a change in the functioning of the industry required the use of a new approach, taking into account the dynamic variability in time, and thus references to the processes performed, and not the functions performed. The concept of the process was defined based on the systems engineering achievements (e.g. Klir 1991), which allowed the transition from reactive to active reaction to changes (sometimes unexpected and fast). The problem prevailing in this phase was the conflict between striving for full flexibility in adapting to the ever faster changing market requirements (so-called responsiveness) and rising costs.

The next stage of logistics development was dominated by the introduction of the supply chain concept as a sequence of processes related to the flow of goods across the borders of individual organizations, ranging from acquiring raw materials to the final user of a given goods. Such a change of perspective in relation to logistics issues enabled a comprehensive approach to the optimization of logistics systems and processes, regardless of the ownership structure of individual parts of the supply chain, and the transition from flexibility in supply management to its higher level—agility. The integration of logistic systems and processes has become the foundation for further stages of the modern logistics development.

The fifth stage started with the beginning of the twenty-first century, and was forced by the ever-expanding economic globalization. Optimization methods based on the concept of M. Porter’s value creation chain to improve the efficiency of logistics systems and a dynamic approach in modelling and simulation of logistics processes have been used on a larger scale. At the same time, the virtualization of logistics networks within the so-called 3rd IT platform, which is often described as the acronym SMAC (Social, Mobile, Analytics, Cloud). This trend, popularly known as e-logistics, fits in fully with the currently developed model of the economics of the moment (so-called ‘now economy’), and implemented mainly in the real-time organizations (RTE—Real-Time Enterprise). The goals of modern logistic systems are multiple, namely effectiveness, economic efficiency, leanness and at the same time agility (so-called ‘leagility’) and resilience to disruptions (Bukowski 2014).

Therefore, the challenges facing modern logistics result from the trends in the development of new technologies, especially information and communication technologies (ICT), 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 (Continuous Improvement Process—CIP), with particular emphasis on risk aspects. The most important directions of activities improving the functioning of modern supply chains and networks can include (based on Pfohl 2016):

- Increasing financial liquidity through active management of working capital (inventories, receivables and financial liabilities);
- Reorientation of supply chains from the perspective of supply to the perspective of demand, through flexible response to market needs (so-called Demand Driven Supply Chain—DDSC);
- Consolidation and all at once regionalization of supply networks, allowing for a significant reduction in transport costs and the number of warehouses;
- Improving the safety and security of the supply network by reducing their vulnerability to external threats related to both the forces of nature (natural disasters), as well as the deliberate actions of criminal or terrorist groups;
- Increasing the resilience of the supply network to threats and hazards as well as the ability to maintain the continuity of supply in crisis conditions (survivability);
- Strategic and comprehensive approach to risk management in supply networks as a tool supporting key logistics decisions.

From the above statement, it is clear that the problems related to operational risk and 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; Coyle et al. 2003; Gudehus and Kotzab 2009; Harisson et al. 2014; Lasch 2014; Nyhuis and Wiendal 2009; Pfohl 2010, 2016; Schönsleben 1998; Shapiro 2001; Stock and Lambert 2001). The submitted work aims to partially fill this gap and build the basis for further exploration of this important issue.

1.2 Defining the Key Terms in Logistics

We assume that the term ‘logistics’ should be qualified to a set of concepts describing the fields of knowledge. Therefore, we propose the following general definition of logistics:

Logistics is a transdisciplinary field of scientific knowledge concerning effective and efficient implementation of flows (movement and storage) of tangible and intangible assets (goods, persons, transactions, and related information) within systems composed of enterprises, their clients and other stakeholders.

The subject of interest in logistics understood in this way are mainly logistics systems and logistics processes (Bukowski 2016). The *logistics system (LS)* is a spatially complex structure, consisting of individual objects connected together (e.g. subsystems), characterized by certain permanent behaviours (e.g. fulfilled functions), within which specific logistic processes are implemented. The *logistics process (LP)* is a sequence of events and actions connected with mutual relationships of the type of flows, aimed at moving and storing material and non-material resources (goods, persons, transactions, and related information).

Logistics systems are often identified with the notion of so-called *logistics infrastructure* and are characterized primarily by structural and spatial complexity. Logistic processes are characterized above all by time extension. The *logistics network (LN)* is a network organization consisting of logistic infrastructure and logistic processes implemented within it. A special case of the logistics network is the *supply chain (SC)*, which is characterized by central coordination of flows and the process of integration of suppliers and recipients initiated by the dominant entity of the organization. In practice the supply chain is understood as the total sequence of business processes, within a single or multiple enterprise environments, that enable customer demand for a product or service to be satisfied.

If a supply system is in direct response to a single point of demand, and all components across a supply chain are synchronized to meet the demand that it is trying to fulfil, then we are dealing with *demand driven supply chains (DDSC)*. In this type of supply chains, the *pull system* is used, where orders for an end item are pulled through the facility to satisfy demand for the end item. An example of pull system is the JIT Kanban process (so-called ‘zero-inventories’ principle). In traditional supply chains the *push system* was used, where orders are issued for completion by specified due dates, based on estimated lead-times, or where the flow of material in a product structure is controlled and determined by the lower levels.

Supply chain management (SCM) is an organisation of the overall business processes to enable the profitable transformation of raw materials or products into finished goods and their timely distribution to meet customer demand. *Raw material* is a stock or items purchased from suppliers, to be input to a production process, and which will be subsequently modified or transformed into finished goods. The stock held to protect against the differences between forecast and actual consumption, and between expected and actual delivery times of procurement orders, to protect against stock-outs during the replenishment cycle is called *safety stock (SS)*. In calculating safety stock, account is taken of such factors as service level, expected fluctuations of demand and likely variations in lead time.

Supply chain sustainability (SCS) is the management of environmental, social and economic impacts and the encouragement of good governance practices, throughout the lifecycles of goods and services. The objective of supply chain sustainability is to create, protect and grow long-term environmental, social and economic value for all stakeholders involved in bringing products and services to market.

A necessary element of modern supply networks are systems that provide them with full *traceability*. It depends on the identification of goods and materials used in

manufacturing or processing to enable the relevant production batch and material source to be traced in case of subsequent defects or complaint.

For more information on terms useful in the logistics area, see Appendix and in Supply Chain and Logistics Terms and Glossary (2010).

References

- Albjoren JS, Haldorson A (2002) Logistics knowledge creation: reflections on content, context and processes. *Int J Phys Distrib Logist Manage* 1
- Blanchard BS (2015) Logistics engineering and management. Pearson Education
- Bukowski L (2014) Core fundamentals of total logistic management. In: Proceedings of VII-th international scientific and technical conference “logistic systems—theory and practice”, OWPW, Warszawa, pp 38–40
- Bukowski L (2016) Ensuring continuity of delivery in a changing and uncertain environment (in Polish). WN WSB, Dąbrowa Górnicza
- Bukowski L (2017) Evolution of logistics concepts in business practice—toward a unified theory (in Polish). *Przedsiębiorczość i Zarządzanie*, Tom XVIII, Nr 8/I: 83–95, ISSN 2543-8190
- Coyle JJ, Bardi EJ, Langley CJ Jr. (2003) The management of business logistic: a supply chain perspective, 7th edn. South-Western, Mason
- 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
- Jünemann R (1989) Materialfluss und Logistik. Springer
- Kirsch W, Bamberger I, Gabele E, Klein HK (1973) Betriebswirtschaftliche Logistik—Systeme, Entscheidungen, Methoden. Gabler, Wiesbaden
- Klir GJ (1991) Facets of systems science. Plenum, New York
- Kovacs G, Spens KM (2007) Logistics theory building. The ICAI University Press
- Lasch R (2014) Strategisches und operatives Logistikmanagement: Prozesse. Springer Gabler, Wiesbaden
- Mangan J et al (2004) Combining quantitative and qualitative methodologies in logistics research. *Int J Phys Distrib Logist Manage* 7(2004):565–578
- Mentzer JT et al (2004) Toward a unified theory of logistics. *Int J Phys Distrib Logist Manage* 8 (2004):606–627
- Morgenstern O (1955) Note on the formulation of the theory of logistics. *Nev Res Logist Quart* 5:129–136
- Nyhuis P, Wiendal H-P (2009) Fundamentals of production logistics. Theory, tools and applications. Springer-Verlag, Berlin Heidelberg
- Pfohl H-CH (2010) Logistiksysteme: Betriebswirtschaftliche Grundlagen. 8. Auflage. Springer, Berlin/Dordrecht/London/New York. ISBN 978-3-642-04161-7
- Pfohl H-CH (2016) Logistikmanagement: Konzeption und Funktionen. 3. Auflage. Springer-Verlag, Berlin Heidelberg. ISBN 978-3-662-48783-9
- Schönsleben P (1998) Integrales Logistikmanagement. Planung und Steuerung von umfassenden Geschäftsprozessen. Springer-Verlag, Berlin Heidelberg
- Shapiro JF (2001) Modelling the supply chain. Thomson Learning, Duxbury
- Shook CL et al (2009) Towards a theoretical toolbox for strategic sourcing. *Supply Chain Manage Int J* 1:3–10
- Stank TP, Pellathy DA, In J, Mollenkopf DA, Bell JE (2017) New frontiers in logistics research: theorizing at the middle range. *J Bus Logist* 38(1):6–17

- Stock JR, Lambert DM (2001) Strategic logistics management. McGraw-Hill Higher Education
- Supply Chain and Logistics Terms and Glossary (2010) http://www.iwla.com/assets/1/24/2010_Glossary_of_Terms_10.7.11.pdf
- Wieland A, Handfield RB, Durach CF (2016) Mapping the landscape of future research themes in supply chain management. *J Bus Logist* 37(3):205–212

Chapter 2

Assessment Knowledge About Engineered Systems



Have no fear of perfection—you'll never reach it.

Salvador Dali

2.1 Concept of Imperfect Knowledge

2.1.1 *From Knowledge Pyramid to Imperfect Knowledge Chain*

Gaining the knowledge necessary for human activity, both in the engineering and management zone, is based on the process of cognition. Aristotle described this process in *Metaphysics* (Irwin 1988) and identified three main interrelated levels: experience, knowledge, and wisdom. In reference to this concept, in the second half of the twentieth century a model of '*The pyramid of knowledge hierarchy*' was created, in which the level of 'experience' was divided into two elements: data and information, and the other two levels—knowledge and wisdom—remained unchanged (Ackoff 1989). This model has become the foundation of a dynamically developing concept of the knowledge management, and has undergone a number of interpretative modifications.

The pyramid of knowledge is based on data that usually occur in the form of symbols and represent individual observations of real world states. *Data* represent raw facts, events, or statements without reference to other things. It does not have a meaning of itself. Usually data is understood as atomistic tiny packets that have no inherent structure. Data can be measurable or not, analogue or discrete, as well as considered statically (e.g. data record) or dynamically (e.g. data stream). It can be obtained from various sources.

Information is data that are processed to be useful, it means data that has been given meaning (e.g. relational connection), relevance and purpose. Information is partly subjective because it depends not only on the data, but also on the process of their interpretation, which is based on the knowledge held by the interpreter at that time. Thus, it can be assumed that information is a collection of selected data, processed and presented in a form that can be useful to the recipient (e.g. the

decision maker). The basic condition for the usefulness of information is its ability to be interpreted in a specific context. In practice this means using the information to find answers to simple questions like: who?, what?, where? and when?. These dependencies can be illustrated by the Langenfor's model, which represents the following relation, called the infological equation (Skyttner 2008):

$$I = i(D, K, t) \quad (2.1)$$

where:

- I information achieved by an interpretation process,
- i an interpretation process acting on data,
- D available data,
- K previous knowledge,
- t available time.

Therefore information is a relation, it means that without a context there is no difference between information and noise. It is an abstract term, and so information per se is something imperceptible. Information can be structured according to the following: alphabet order, content category, continuum (continuous or discontinuous), location and time.

Knowledge is created by integrating new information with existing knowledge about a particular area of interest. It requires the ability to evaluate available information and understand reality in light of this information, in accordance with the current state of knowledge. Knowledge relies on the ability to use information effectively and efficiently to find answers to more complex questions, such as 'how?'. Knowledge is emergent in relation to information—it is possible to generate new knowledge by applying processes of systematization and structuring of information.

Wisdom is the ability to make effective use of your knowledge and experience. In other words it is:

- ability to make legitimate decisions that bring positive results in the future,
- wide and deep knowledge combined with intelligence and maturity,
- ability to understand the world, phenomena and relationships between them.

Thus, the notion of wisdom places itself at the edge of many scientific disciplines, including philosophy.

The interdependences between all four categories: data, information, knowledge and wisdom, are shown in Fig. 2.1 in the form of the modified knowledge pyramid. The modification allows us to assess qualitatively the degree of usability for each category and, additionally, to take into account the quantity of units in each category (the number of units in each category is proportional to the area representing this category). This model has a static nature and can be interpreted as a hierarchical metaphor of the relationship between the various elements of the cognition process. The process approach to these relations, however, is shown in Fig. 2.2. Filtering and aggregation of disparate pieces of data, and next understanding the relationship

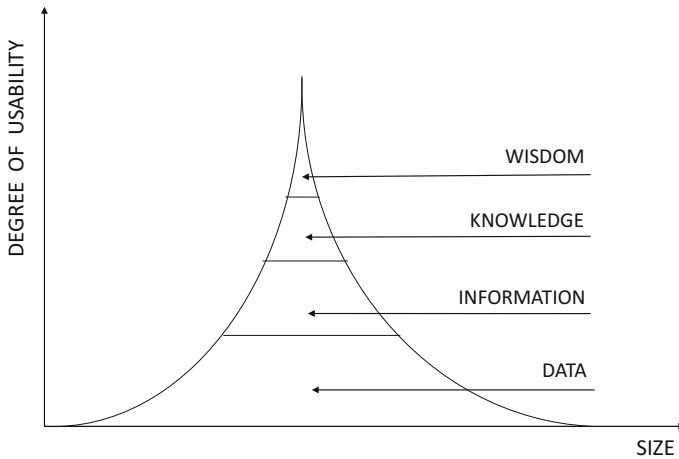


Fig. 2.1 The modified version of knowledge pyramid model

between individual data allows to give them a certain context, so that they are transformed to the level of information. Accumulation and assimilation of multiple pieces of information, as well as understanding the patterns existing in the set of information, allows us to give them a certain meaning, so that they are transformed to the level of knowledge. Finally, understanding the rules and functional principles governing the knowledge system allows them to be useful in decision-making, so that they are transformed to the level of wisdom.

The models shown in Figs. 2.1 and 2.2 illustrate the general relationship between the different categories of knowledge pyramid, without taking into account the uncertainty aspect. This approach corresponds to the notion of the perfection of all processes in the knowledge chain, which in practice is impossible to achieve. In 1957, Bergmann published his work, *Philosophy of science*, in which he made a distinction between ‘perfect’ and ‘imperfect’ knowledge. Perfect knowledge is based on complete theories, deterministic nature laws (such as Newtonian mechanics); it concerns closed systems in which the initial conditions are known accurately, and the only method used in the inference is the deductive method.

Whereas, in applied sciences such as engineering, social sciences, economics or management, knowledge is based on incomplete theories and indeterministic laws. It concerns open systems in which the initial conditions are known inaccurately, and the method used in the inference is usually the inductive method—it is therefore imperfect. The data on which the entire pyramid is built come from observations or measurements whose accuracy is limited and therefore burdened with errors. If it is possible to repeat the same observations or measurements, the use of statistical methods minimizes the impact of these errors on our knowledge. But in many cases there is no such possibility, and then we have to settle for knowledge of the high imperfection degree.

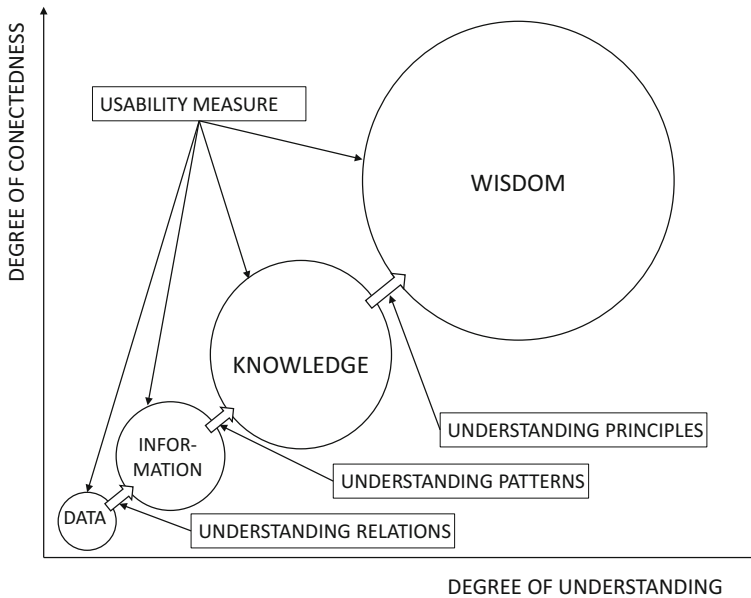


Fig. 2.2 The modified version of knowledge chain model

2.1.2 Data and Information Imperfection

The problem of *knowledge imperfection* has become particularly important as a result of the avalanche increase of access to vast amounts of data, called ‘Big Data’ (Corrigan 2013). *Big data* includes data sets with sizes beyond the ability of software tools commonly used to capture, manage, and process data within an acceptable period of time. Big data can be described by the following characteristics (‘10Vs’ model for describing big data):

- **Volume**—represents how much data we have. It refers to the huge amount of data being generated. The Internet of Things is creating exponential growth in data, and what used to be measured in Gigabytes is now measured in Zettabytes or even Yottabytes.
- **Velocity**—is the speed in which data is accessible. It refers both to the increasing rate of data sets and constantly growing demand for access to databases.
- **Variety**—refers to different types of data. It can be structured, semi-structured as well as unstructured, and it can include many different kinds of data such as numbers, messages, photos, sensor data, voice or video. Organizing the data in a meaningful way is demanding task, especially when the data itself changes rapidly.
- **Variability**—is different from variety. If the meaning of data is changing in time it can have a huge impact on data homogenization.

- Visualization—is more and more important in today's world. Using charts and graphs to visualize big amounts of complex data is much more effective in meaning communication than spreadsheets and reports with numbers and formulas.
- Veracity—refers to truthfulness and reliability of data. Highly complex data sets contain significant amounts of dubious data (data in doubt), which constitutes database imperfections.
- Value—is the advantage that the data can bring to the owner.
- Validity—refers to how accurate and correct the data is for its intended use.
- Volatility—refers to how old does the data be before it becomes irrelevant.
- Vulnerability—refers to how secure the data is for its safe use.

What has the decisive influence on the degree of knowledge imperfection is the *data veracity*. It depends on the imperfection of the data, whatever the reason for it, due to (Klir 1987): incorrectness, incredibility, implausibility, inconsistency, incoherency, vagueness, ambiguity, incompleteness, imprecision and inaccuracy. Based on the literature (e.g.) and the author's own experiences, the following definition of data veracity is proposed.

Data Veracity (DV) is the property of the data described by five-dimensional vector of its attributes:

- Accuracy (ACC)—the degree to which the data fulfils the relevant requirements (the data should precisely meet certain specifications and standards).
- Clarity (CLA)—the degree to which the data can be clearly understood (the data should be well defined, without several meanings, vagueness and ambiguity).
- Consistency (CON)—the degree to which the data is compatible with the same type of data from different sources (the data should be coherent without confusing or conflicting meaning).
- Plausibility (PLA)—the degree to which the data is fitted to reality (the data should be compatible with reality, imaginable and possible).
- Traceability (TRA)—the degree to which the data can be traced to its sources (the origin of the data should be ascertained with confidence).

This definition can be illustrated by the model, which represents the following relation

$$DV = \{ACC, CLA, CON, PLA, TRA\} \quad (2.2)$$

In order to use this model to assess the data veracity, we propose the following expert method. Each veracity attribute A_i is rated on a 3-point scale as:

- 0—unacceptable,
- 1—acceptable,
- 2—fully satisfactory,

and on this basis, the *Data Veracity Value (DVV)* is calculated as the product of all five attributes A_i .

$$DVV = \prod_{i=1}^5 A_i \tag{2.3}$$

The result of the assessment is to assign them to one of five classes, namely:

- Rank 0—very low (VL) unacceptable,
- Rank 1 to 2—low (L),
- Rank 4 to 8—moderate (M),
- Rank 16—high (H),
- Rank 32—very high (VH).

Data for which Data Veracity Value is very low ($DVV = 0$) should be eliminated and must not be used to create information. An example of using this method to evaluate data veracity is shown in Table 2.1. In this case the analysed data veracity was assessed as ‘moderate’.

Uncertainty of information may be due to objective reasons caused by data imperfections and subjective errors caused by errors in their interpretation. In practice, objective reasons generally predominate, so the uncertainty of the information is largely determined by the quality of the data held. Therefore, their interpretation and, in particular, the elimination of false and contradictory data, and their definition in case of data ambiguity, are of great importance in the process of acquiring information. Furthermore, the uncertainty of the information must be assessed on the basis of the available data on the required completeness, accuracy and relevance. The degree of information uncertainty determines its quality and usefulness for creating new knowledge.

The most common dimensions of *information quality* are following:

- Accessibility—extent to which information is available, or easily and quickly retrievable.
- Accuracy—extent to which data are correct, reliable and free of error.
- Amount of data—extent to which the quantity or volume of available data is appropriate.
- Availability—extent to which information is physically accessible.
- Believability—extent to which information is regarded as true and credible.
- Completeness—extent to which information is not missing and is of sufficient breadth and depth for the task at hand.

Table 2.1 An example of data veracity value assessment

Data veracity attributes A_i	0	1	2	Rank
A_1 —Accuracy (ACC)			x	2
A_2 —Clarity (CLA)			x	2
A_3 —Consistency (CON)		x		1
A_4 —Plausibility (PLA)			x	2
A_5 —Traceability (TRA)		x		1
Data veracity value (DVV) = $\prod_{i=1}^5 A_i$				8

- Concise—extent to which information is compactly represented without being overwhelming (i.e. brief in presentation, yet complete and to the point).
- Consistency—extent to which information is presented in the same format and compatible with previous data.
- Efficiency—extent to which data are able to quickly meet the information needs for the task at hand.
- Navigation—extent to which data are easily found and linked to.
- Objectivity—extent to which information is unbiased, unprejudiced and impartial.
- Relevancy—extent to which information is applicable and helpful for the task at hand.
- Reliability—extent to which information is correct and reliable.
- Reputation—extent to which information is highly regarded in terms of source or content.
- Security—extent to which access to information is restricted appropriately to maintain its security.
- Timeliness—extent to which the information is sufficiently up-to-date for the task at hand.
- Understandability—extent to which data are clear without ambiguity and easily comprehended.
- Usability—extent to which information is clear and easily used.
- Usefulness—extent to which information is applicable and helpful for the task at hand.
- Value-Added—extent to which information is beneficial and provides advantages from its use.

In practice, the quality of information is conditioned by the context in which it is used. Therefore, in the decision-making process it is essential to evaluate the usefulness of information as its quality in the context of the specific purpose of its use. Based on the literature (Kulikowski 2014) we propose the introduction of the term *information utility* as an equivalent of the usefulness of information, and the following definition of the term.

Information Utility (IU) is the property of the information described by five-dimensional vector of its attributes:

- Believability (BEL)—the degree to which the information can be reliable (the information should be: believable, of undoubtful credibility and from the reputable source).
- Completeness (COM)—the degree to which the information does not contain omission errors (the information should: include all the necessary values, be complete, cover the needs of our tasks and have sufficient breadth and depth).
- Correctness (COR)—the degree to which the information is proper (the information should be free from errors).

- Relevancy (REL)—the degree to which the information is useful (the information should be: relevant and applicable to our work, as well as appropriate for our needs).
- Timeliness (TIM)—the degree to which the information is up to date (the information should be sufficiently: timely, current for our work and fresh enough for our needs).

This definition can be illustrated by the model, which represents the following relation

$$IU = \{BEL, COM, COR, REL, TIM\} \quad (2.4)$$

In order to use this model to assess the Information Utility, we propose the following expert method.

Each IU attribute B_i is rated by experts on a 3-point scale as:

- 1—low,
- 2—moderate,
- 3—high,

and on this basis, the *Information Utility Value* (IUV) is calculated as the product of all five attributes B_i .

$$IUV = \prod_{i=1}^5 B_i \quad (2.5)$$

The result of the assessment is to assign them to one of five classes, namely:

- Rank 1 to 4—very low (VL),
- Rank 6 to 12—low (L),
- Rank 16 to 48—moderate (M),
- Rank 72 to 108—high (H),
- Rank 162 to 243—very high (VH).

An example of using this method to evaluate data veracity value is shown in Table 2.2. In this case the analysed data veracity was assessed as ‘moderate’.

Table 2.2 An example of information utility value assessment

Information utility attributes B_i	1	2	3	Rank
B_1 —Believability (BEL)		x		2
B_2 —Completeness (COM)			x	3
B_3 —Correctness (COR)		x		2
B_4 —Relevancy (REL)			x	3
B_5 —Timeliness (TIM)	x			1
Information utility value (IUV) = $\prod_{i=1}^5 B_i$				36

2.1.3 The Process of Knowledge Creating and Managing

The imperfection of knowledge is due to the uncertainty of the information obtained and the imperfection of the process of integrating this information with the knowledge of the area. The general model of knowledge creating process is shown in Fig. 2.3. The entire process is presented as a chain of operations and flows that are subjected to disturbances. The raw data stored in block I (Data Acquisition) is sent to block II (Data Processing) and subjected to the preparation process. The processed data flows to block III (Data Verification) where they are verified for their veracity (VER) and then sent to block IV (Data Forming) for information generation (Data Mining and Fusion of Data). Raw information flows to block V (Information Evaluating), where they are evaluated for their utility value (IUV) and selected on this basis. The selected information is used in block VI (Building Patterns) to look for relationships between individual pieces of information and build logical patterns, based on which a new knowledge is generated in block VII (New Knowledge Creation). The last stage of the chain (block VIII) is to enrich the existing knowledge base with new knowledge and to create initial knowledge for further acquisition of new data.

In order to ensure the quality of the information on which the new knowledge is created, the process of data preparation is of particular importance; thus it will be described in more detail. In data processing step four main tasks may be differentiated: data cleaning, data integration, data transformation, and data reduction. Below follows a description of the typical procedures involved in these tasks (e.g. based on Al Shalabi et al. 2006).

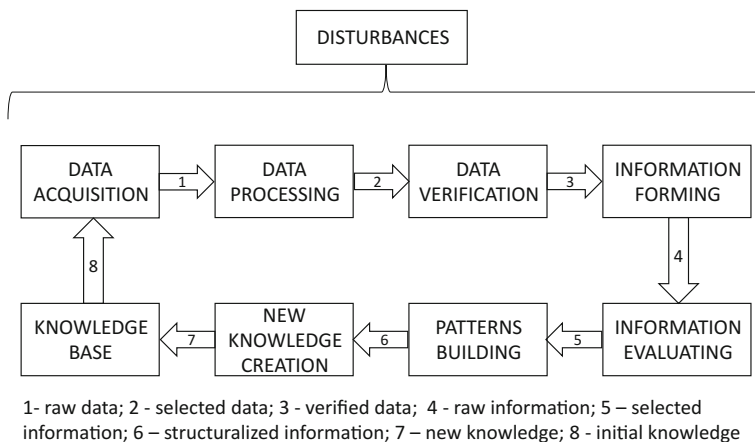


Fig. 2.3 The process of knowledge creating

(a) Data cleaning

The data cleaning task involves three operations, which can be supported by algorithmised methods:

- replacement of missing or empty values by calculated numbers with the use of the remaining attribute values,
- accuracy improvement through the replacement of the current value with the newly-calculated one or through the removal of this current value,
- inconsistency removal through special procedures (e.g. control codes) programmed in data collection sheets.

(b) Data integration

For knowledge extraction it is necessary to represent the data in the form of a flat, two-dimensional table, because the column–row structure—as in a calculation sheet—is the most useful one. At this stage, the operations are performed with the following procedures:

- identification by recognising the attributes which could not have been identified at the cleaning process,
- redundancy removal by comparing the attributes values with the aim of removing the redundant data,
- unification of the data collected in different sets with the same form, for instance the same units.

(c) Data transformation

Data transformation encompasses all the issues connected with transforming the data into a form which makes data exploration possible, and involves six operations:

- smoothing by elimination of the local data deviations having the character of noise. Smoothing encompasses the techniques, such as binning, clustering, or regression,
- aggregation by summing up the data, most frequently in the function of time,
- generalization by converting the collected data into higher-order quantities, for instance via their discretization,
- normalization by the rescaling (adjustment) of the data to a specified, narrow range, for example, from 0 to 1,
- attribute construction by mathematical transformations of attributes with the aim of obtaining a new attribute, which will replace its constituent attributes in modelling,
- accommodation by transforming the data into a format used by a specific algorithm or a tool.

(d) Data reduction

Attribute selection with the expert opinion and experience pertaining to the data under analysis, that one can remove from the set of collected data. Therefore, those attributes which do not have any influence on the features under modelling. The aim of the data reduction techniques is a significant decrease in the data quantity. Data reduction includes five operations:

- attribute selection by eliminating the attributes which are redundant or have little significance for the phenomenon under modelling,
- dimension reduction through transforming the data with the aim of arriving at a reduced representation of the basic data,
- size reduction by eliminating the recurring or similar cases,
- discretization through transforming a continuous variable into a limited and specified number of ranges,
- aggregation by summing up the data.

The created knowledge is the basis for the decision-making process, therefore the greater the imperfection of knowledge, the greater the risk related to decision-making. Moreover, the following additional factors can have impact on the level of risk: imperfections in communication processes in the system (reliability of information flow), and imperfections in decision realization processes. All these elements can be included in the area of imperfect knowledge managing.

The general model of imperfect knowledge managing is shown in Fig. 2.4. The entire process is presented as a sequence of operations and flows that are subjected to different disturbances. The knowledge stored in block I (Knowledge Base) is sent to block II (Model Building) and forms the basis for choosing the right type of decision model. The information about the chosen model type flows to block III (Parameter Evaluation) in which, based on the background knowledge, parameters

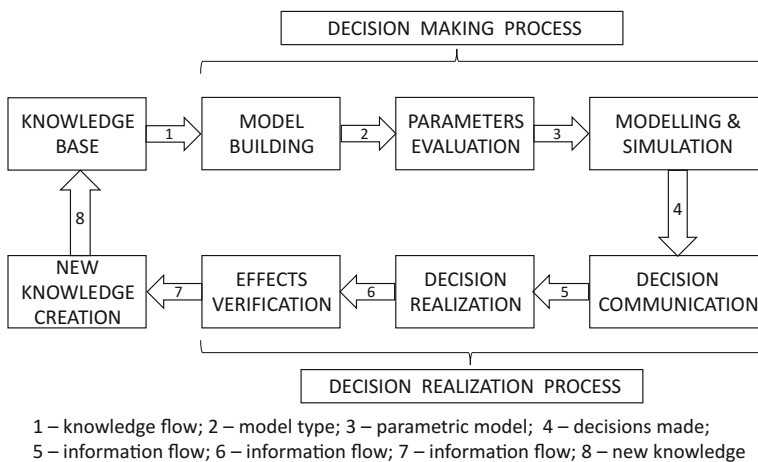


Fig. 2.4 The process of imperfect knowledge managing

of the chosen model are determined and then sent to block IV (Modelling and Simulation). In this block, appropriate investigations are carried out on the parametric model in order to find the best possible decision, and then the decision made flows to block V (Decision Communication). In the next step the information about the decision flows to block VI (Decision Realization), and after the decision realization into block VII (Effects Verification). In this block the results of the decision taken are checked, conclusions for the future drawn and a piece of new knowledge in block VIII (New Knowledge Creation) is generated. The last stage of the chain is to enrich the existing knowledge base (block I) with the new knowledge and to create initial knowledge for further decision making.

Based on the concept of imperfect knowledge creating and managing process we propose to describe *Knowledge Processing Quality (KPQ)* using five-dimensional vector of its attributes as follows:

- Model Type Adequacy (MTA)—the ability to reflect the reality with sufficient plausibility and sensibility,
- Model's Parameters Accuracy (MPA)—the ability to reflect the reality with sufficient precision,
- Decision Making Process Correctness (DMC)—the ability to make decisions without significant errors,
- Decision Communication Process Reliability (DCR)—the ability to communicate decisions without faults,
- Decision Realization Process Compliance (DRC)—the ability to carry out decisions in accordance with the intention of the decision maker.

This definition can be illustrated by the model, which represents the following relation

$$KPQ = \{MTA, MPA, DMC, DCR, DRC\} \quad (2.6)$$

In order to use this general model of imperfect knowledge managing (2.6) for assessing knowledge processing quality (KPQ), we propose the following expert method.

Each KPQ attribute C_i is rated by experts on a 3-point scale as:

- 1—low,
- 2—moderate,
- 3—high,

and on this basis, the value of the *Knowledge Processing Quality (KPQ)* is calculated as the product of all attributes C_i .

$$KPQ = \prod_{i=1}^5 C_i \quad (2.7)$$

Table 2.3 An example of knowledge processing quality assessment

Knowledge processing quality attributes C_i	1	2	3	Rank
C_1 —Model adequacy (MA)			x	3
C_2 —Parameter accuracy (PA)		x		2
C_3 —Decision correctness (DC)		x		2
C_4 —Communication reliability (CR)			x	3
C_5 —Realization compliance (RC)		x		2
Knowledge processing quality (KPQ) = $\prod_{i=1}^5 C_i$				72

The result of the assessment is to assign them to one of five classes, namely:

- Rank 1 to 4—very low (VL),
- Rank 6 to 12—low (L),
- Rank 16 to 48—moderate (M),
- Rank 72 to 108—high (H),
- Rank 162 to 243—very high (VH).

An example of using this method to evaluate Knowledge Processing Quality is shown in Table 2.3. In this case the analysed KPQ was assessed as ‘high’.

2.1.4 Knowledge Maturity Assessment

Maturity model describes how an entity develops through the levels over time until it reaches the highest level. Maturity models have the following properties (Klimko 2001; Weerdmeester et al. 2003):

- The development of a single entity is simplified and described with a limited number of maturity levels (usually four to six).
- Levels are characterized by certain requirements, which the entity has to achieve on each level.
- Levels are ordered sequentially, from an initial level up to an ending level (the latter is the level of perfection).
- During development, the entity progresses forward from one level to the next, therefore no levels can be skipped.

MITRE (2014) has designed a maturity model of knowledge management organized into five maturity levels:

- I. Initial Level—the knowledge process is ad hoc and chaotic. Partial technical infrastructure exists to support knowledge discovery and sharing.
- II. Repeatable Level—basic knowledge management program is established to track requirements, content and investments. Process discipline is in place to assure quality of knowledge and/or to repeat earlier knowledge successes

- and/or knowledge transfer on similar projects ensuring some basic knowledge quality and reuse. A knowledge focal point is identified.
- III. Defined Level—at this level, the process for both knowledge management and knowledge engineering activities is documented. Processes are standardized across the organization. Manual or semi-automated methods for mapping knowledge are applied and available across the enterprise. Training and inter-group coordination is used for knowledge discovery and dissemination.
 - IV. Managed Level—detailed measures of the knowledge process and product quality are collected. Both the knowledge process and products are quantitatively understood and controlled.
 - V. Optimizing Level—continuous process improvement is enabled by quantitative feedback from the process and from piloting innovation. Knowledge management activities are closely aligned with business functions.

We propose using the concept of maturity to assess knowledge that is available when making decisions under risk conditions. Assessment of the *knowledge maturity* (KM) should be based on three basic criteria, namely: data veracity value (five levels), information utility value (five levels) and knowledge processing quality (five levels). Methods for determining these criteria are described in Sects. 2.1.2 and 2.1.3. This definition can be illustrated by the model, which represents the following relation:

$$KM = \{DVV, IUV, KPQ\} \quad (2.8)$$

Each KM attribute D_i is rated on a 5-point scale, and on this basis, the value of the *Knowledge Maturity Level* (KML) is calculated as the product of all attributes D_i .

$$KML = \prod_{i=1}^3 D_i \quad (2.9)$$

Maturity of knowledge can also be assessed on five levels, e.g.:

- Rank 2 to 4—very low (insufficient) maturity level (VL),
- Rank 8 to 18—low maturity level (L),
- Rank 27 to 48—moderate maturity level (M),
- Rank 64 to 80—high maturity level (H), and
- Rank 100 to 125—very high (fully satisfactory) maturity level (VH).

Very low (VL) maturity level can be identified with a lack of knowledge, the level L—weak imperfect knowledge, the level M—medium imperfect knowledge, the level H—strong imperfect knowledge, and the level VH—complete, perfect knowledge.

An example of using this method to evaluate Knowledge Maturity Level (KML) is shown in Table 2.4. In this example the analysed KML was assessed as ‘moderate maturity level’.

Table 2.4 An example of knowledge maturity level assessment

Knowledge maturity attributes D_i	VL = 1	L = 2	M = 3	H = 4	VH = 5	Rank
D_1 —DVV			x			3
D_2 —IUV			x			3
D_3 —KPQ				x		4
Knowledge maturity level (KML) = $\prod_{i=1}^5 D_i$						36

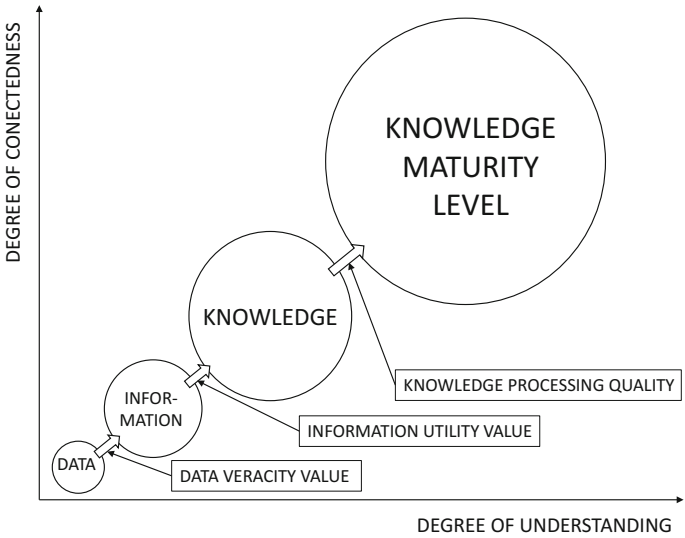


Fig. 2.5 The process of knowledge maturity assessment

The whole process of assessing the maturity of knowledge based on imperfect data, information and knowledge processing can be presented in the form of Fig. 2.5.

2.2 Uncertainty Modelling

2.2.1 General Concept of Uncertainty

The consequence of knowledge imperfections is, among other things, the uncertainty in the decision-making process. We will understand the concept of uncertainty as a situation of having limited, imperfect knowledge such as:

- The order, nature or state of things is unknown, and
- The consequence, extent, or magnitude of circumstances, conditions, or events is unpredictable.

There are many forms of uncertainty, but the most common is its division into two categories: aleatory and epistemic uncertainty (Eusgeld et al. 2008). The aleatory uncertainty is understood as an inherent variation associated with the engineered system or the environment under consideration. It can be observed in random experiments and described by probability distributions. Traditional reliability engineering and risk analysis applications tend to model only the aleatory uncertainties, which can lead to significant underestimations of the real risks and overestimation of reliability. However, the epistemic uncertainty is not an inherent property of the system or its environment, and it results from our inability to understand as well as describe and model reality. Thus, in this case the standard probabilistic methods are not useful.

In 2005 Lotfi A. Zadeh proposed *a generalized uncertainty theory* (GTU), which attempts to unify the approach to uncertainty. The GTU theory was based on the concepts of granular structures and generalized constraints. The basic assumptions of these concepts are illustrated in Fig. 2.6. Let X be a variable taking values in a universe of discourse, U , then a is a singular value of X (e.g. a singleton), implying that there is no uncertainty about the value of X . If this is not the case, then a granular value of X , A , may be viewed as a representation of the state of knowledge about the value of X .

Informally, a granule of a variable X is a clump of values of X which are drawn together by indistinguishability, equivalence, similarity, proximity or functionality. For example, intervals (crisp or fuzzy) are granules, as well as different probability distributions (Bargiela and Pedrycz 2002). The concept of granularity underlies the concept of a linguistic variable—a concept which was introduced by Zadeh (1973)

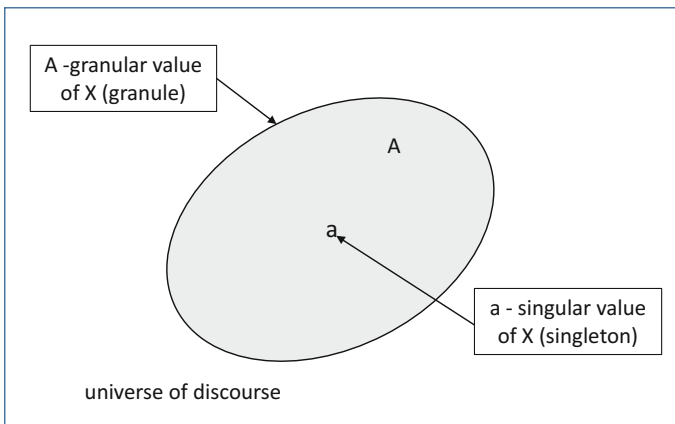


Fig. 2.6 Singular and granular values

in the paper “Outline of A New Approach to the Analysis of Complex Systems and Decision Processes”. The concept of a linguistic variable plays a pivotal role in many applications of fuzzy logic (Dubois and Prade 1996; Filev and Yager 1994; Jamshidi et al. 1997; Pedrycz and Gomide 1998; Ross 2004; Yen and Langari 1998). There are four basic rationales which underlie granulation of attributes and the use of linguistic variables:

- the bounded ability of sensory organs to resolve detail and store information,
- when numerical information is not available,
- when an attribute is not quantifiable because we do not have a numerical scale for it,
- when there is an acceptance for imperfection (e.g. inaccuracy or imprecision) which can be exploited through granulation to achieve tractability, and economy of communication.

Figure 2.7 shows the differences between quantized and granulated describing of the variable X , which for example can describe any feature of data veracity or quality of information. Let us assume that these attributes are evaluated by experts on a scale of 1–5. The upper chart shows the evaluation values in the form of singletons (1, 2, 3, 4, and 5) as well as the ranges of quantized values (1.0–1.5, 1.5–2.5, 2.5–3.5, 3.5–4.5, and 4.5–5.0). The bottom graph shows the corresponding granular values of the attribute in the form of triangular fuzzy membership functions for five classes (very low, low, medium, high, and very high). The symbol μ denotes the membership function of the set X .

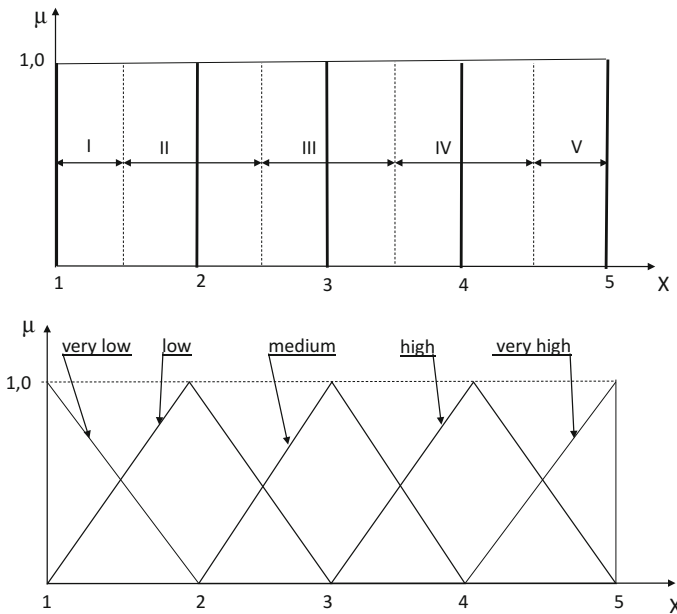


Fig. 2.7 Granulation and quantization of the variable X

There is a close connection between granularity and uncertainty. Suppose X is a variable and we are looking for the value of this variable. If the answer is “ X is a ”, where a is a singleton, then there is no uncertainty in the information about X , because the information is singular. But if the answer is “ X is approximately a ”, in abbreviation “ X is $*a$ ”, then there is some uncertainty in the information, because information is described as granular. Therefore, granularity may be equated to non-singularity. In the context of standard probability theory, $*a$ would normally be interpreted as a probability distribution centred on a . In GTU, information about X is viewed as a generalized constraint on X , or more specifically, as a granule which is characterized by a generalized constraint. A probability distribution can be seen as a special case of a generalized constraint.

A generalized constraint, GC, is defined as an expression of the form (Zadeh 2005):

$$GC : X \text{ isr } R \quad (2.10)$$

where: X is the constrained variable; R is a constraining relation which, in general, is non-bivalent; and r is an indexing variable which identifies the modality of the constraint, that is, its semantics. The variable, X , may have a variety of forms, and in particular:

- X is an n -ary variable, e.g. $X = (X_1, \dots, X_n)$,
- X is a proposition, e.g. $X = \text{Object } z \text{ is medium}$,
- X is a function,
- X is a function of another variable, e.g. $X = f(Y)$,
- X is conditioned on another variable, e.g. X/Y ,
- X has a structure, e.g. $X = \text{AttributeA1}(\text{AttributeA2}(\text{Object } z))$,
- X is a group variable, e.g. there is a group, $G[A]$; with each member of the group, Object_i , $i = 1, \dots, n$, associated with an attribute-value, A_i . A_i may be vector-valued, and $G[A]$ is a relation,
- X is a generalized constraint, $X = Y \text{ isr } R$.

The principal modalities of generalized constraints are summarized in the following.

(a) *Probabilistic* ($r = p$)

$$X \text{ isp } R \quad (2.11)$$

with R —the probability distribution of X . For example:

$$X \text{ isp } N(m, \sigma) \quad (2.12)$$

means that X is a normally distributed random variable with mean m and variance σ^2 .

If X is a random variable which takes values in a finite set $\{u_1, \dots, u_n\}$ with respective probabilities $p_1, \dots, p_n$, then X may be expressed as:

$$X \text{ is } p(p_1 \setminus u_1 + \dots + p_n \setminus u_n) \quad (2.13)$$

with the semantics

$$\text{Prob}(X = u_i) = p_i \quad i = 1, \dots, n \quad (2.14)$$

In GTU a probabilistic constraint is viewed as an instance of a generalized constraint. When X is a generalized constraint, the expression $X \text{ is } R$ is interpreted as a probability qualification of X , with R as the probability of X (Zadeh 2005). For example:

$$(X \text{ is } \textit{big}) \text{ is } \textit{likely} \quad (2.15)$$

It means that the probability of the fuzzy event $\{X \text{ is } \textit{big}\}$ is likely, where “big” is a fuzzy subset of the real line.

(b) *Possibilistic* ($r = \text{blank}$)

$$X \text{ is } R \quad (2.16)$$

with R playing the role of the possibility distribution of X . For example:

$$X \text{ is } [a, b] \quad (2.17)$$

means that $[a, b]$ is the set of possible values of X . Next example:

$$X \text{ is } \textit{small} \quad (2.18)$$

In this case, the fuzzy set labelled small is the possibility distribution of X , and $\mu_{\textit{small}}$ is the membership function of small, then the semantics of “ X is small” is defined by

$$\text{Poss}\{X = u\} = \mu_{\textit{small}}(u) \quad (2.19)$$

where u is a generic value of X .

(c) *Veristic* ($r = v$)

$$X \text{ is } v R \quad (2.20)$$

where R plays the role of a verity (truth) distribution of X . In particular, if X takes values in a finite set $\{u_1, \dots, u_n\}$ with respective verity (truth) values (Nguyen et al. 2003) $t_1, \dots, t_n$, then X may be expressed as:

$$X \text{ is } v (t_1 | u_1 + \dots + t_n | u_n) \quad (2.21)$$

meaning that $\text{Ver}(X = u_i) = t_i, i = 1, \dots, n$.

When X is a generalized constraint, the expression $X \text{ isv } R$ is interpreted as verity (truth) qualification of X . For example:

$$(X \text{ is small}) \text{ isv very.true} \quad (2.22)$$

should be interpreted as “It is very true that X is small.” The semantics of truth qualification is defined in (Zadeh 2005)

$$\text{Ver}(X \text{ is } R) \text{ is } t = X \text{ is } \mu_R^{-1}(t) \quad (2.23)$$

where μ_R^{-1} is inverse of the membership function of R_i and t is a fuzzy truth value which is a subset of $[0, 1]$.

Therefore, there are two classes of fuzzy sets: (b) possibilistic, and (c) veristic. In the case of a possibilistic fuzzy set, the grade of membership is the degree of possibility. In the case of a veristic fuzzy set, the grade of membership is the degree of verity (truth).

There are many ways in which generalized constraints may be operated on. The basic operation is conjunction.

Conjunction

$$\{X \text{ is } R\} \& \{Y \text{ is } S\} \Rightarrow \{(X, Y) \text{ is } T\} \quad (2.24)$$

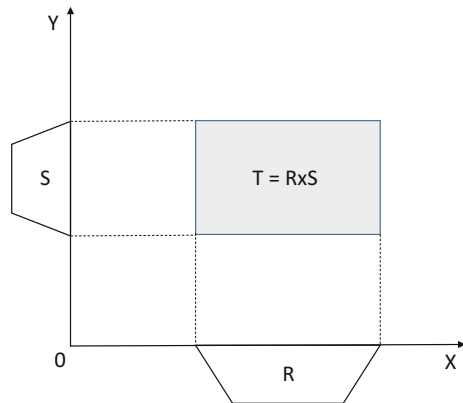
An example with possibilistic constraints is shown in Fig. 2.8, for:

$$\{X \text{ is } R\} \& \{Y \text{ is } S\} \Rightarrow \{(X, Y) \text{ is } R \times S\} \quad (2.25)$$

where X is the Cartesian product.

The three primary constraints: possibilistic, probabilistic and veristic, are closely related to the concept of partiality, which has a central position in human cognition.

Fig. 2.8 An example of possibilistic conjunction



In the sense used here, partial means: a matter of degree, equivalent to fuzzy. Typical examples of fuzzy concepts are the following terms: knowledge, understanding, belief, relevance, truth, likelihood and possibility. Therefore, existing theories of uncertainty may be viewed as theories of different mixtures of primary constraints. For example, the Dempster–Shafer theory of evidence is a theory of a mixture of probabilistic and possibilistic constraints. The generalized theory of uncertainty embraces all possible mixtures, and in this sense the conceptual structure of GTU accommodates most of the existing theories of uncertainty.

2.2.2 *Uncertainty Modelling Methods*

The starting point for considering knowledge uncertainty may be the Generalized Information Theory (GIT), proposed by Klir (2004). Compared to the classical information theory created by Shannon (1948), based on the concepts of probability and entropy, it has a much more universal character. GIT is the result of two significant mathematical generalizations:

- the classical theory of additive measures to the theory of monotonic measures and
- the classical theory of crisp sets to a more general theory of fuzzy sets.

The first generalization, which started in the early 1950s, extends additive measures to less restrictive monotonic measures, characterized by more diverse features. The second one, introduced in the 1960s, expands the language of the classical set theory into a more universal language of fuzzy sets, allowing the use of vague linguistic terms. *The theory of uncertainty of a given type is formed by choosing the appropriate language (e.g. based on the classical set theory or the theory of fuzzy sets), and expressing uncertainty by means of specific monotone measures (e.g. based on the theory of probability or the possibility theory).*

In each types of the theories, uncertainty is represented by the so-called uncertainty function, assigning each possible realization from the set a number from the interval $[0,1]$, which determines the degree of certainty that a specific opportunity arises. Examples of uncertainty functions include: the probability function, the possibility function, the necessity function, the belief measure, the plausibility measure or the lower and upper probabilities. In each theory, the uncertainty function meets certain requirements that differentiate the various theories. The measure of uncertainty for a specific type of theory is the functional that assigns a non-negative real number to each function. Typical examples of uncertainty measures are the Shannon’s entropy (Shannon 1948) and Hartley’s measure (Hartley 1928). A functional representing the uncertainty measure must meet a number of requirements. Admittedly, mathematical formalization of each of the requirements depends on the theory used, however, these requirements can be represented in the general form as:

- additivity—the uncertainty in the total data representations is equal to the sum of uncertainty of individual representations of data,
- subadditivity—the uncertainty in the total representation of data cannot be greater than the total uncertainty of the sum of individual data representation,
- range—the uncertainty is contained in the interval $(0, M)$, where 0 is related to the function that describes the complete certainty and M depends on the size of the set used and the selected unit of measure,
- continuity—the functional representing any uncertainty measure must be continuous,
- expansibility—developing a set of alternatives by adding alternatives cannot change the level of uncertainty,
- consistency—if uncertainty can be calculated in different ways (allowed in the method), the result must be the same,
- monotonicity—if the data form an increasing series, their measure of uncertainty also increases and vice versa, if the data in a series are decreasing, uncertainty also decreases,
- coordinate invariance—a measure of uncertainty cannot change with the isometric coordinate transformations.

These requirements must be fulfilled by all types of uncertainty that exist in the theory.

There are three main principles of uncertainty management:

- the principle of minimum uncertainty—we accept only those solutions for which the loss of information (resulting from simplifications, transformations, and conflict-resolutions problems) is minimal, i.e. we choose solutions with a minimum of uncertainty,
- the principle of maximum uncertainty—we accept all solutions, after making sure that the information that raises doubt is reliable,
- the principle of uncertainty invariance—the level of uncertainty should be kept at each transition from one mathematical approach to another.

2.2.2.1 Formalized Languages

Currently, three formalized languages are used to describe sets: CST—the Classical Sets Theory, SFST—the Standard Fuzzy Sets Theory and NFST—the Nonstandard Fuzzy Sets Theory. The first two theories are thoroughly described in the literature, being well-developed and widely used (e.g. Beer and Möller 2013), while the last one is a relatively new theory and not yet fully developed.

(A) The classical set theory

In the classical set theory, it is assumed that each element of the considered space X belongs to either set A ($x \in A$) defined on the space X ($A \in P(X)$), or it

complements the set A ($x \in \bar{A}$), that is, no element can belong simultaneously to both sets. The characteristic function (membership function) of the set A is

$$m_A : X \rightarrow \{0, 1\} \text{ and } m_A = \begin{cases} 1 & \text{for } x \in A \\ 0 & \text{for } x \notin A \end{cases} \text{ for each } x \in X \quad (2.26)$$

Two sets are equal only when every element of one of them is the element of the other and vice versa. Two sets of the same number of elements are called equinumerous.

The interference based on binary logic and classic sets is simple and unambiguous, but in many cases insufficient to describe the complex reality.

(B) The standard fuzzy sets theory

The concept of fuzzy sets was introduced by Zadeh (1965) as a generalization of the classical set theory. In the case of fuzzy sets, each element of space X can belong partially to a set A , and partly to its complement $\bar{A}$. Fuzzy sets are defined by the membership function corresponding to the function characteristics of classical sets. Each element of the set X has the assigned value that defines the degree of membership to the fuzzy set. The membership function of the standard fuzzy sets belongs to a range $[\alpha, \beta]$ and if we deal with the normal fuzzy sets $\alpha = 0$ and $\beta = 1$. Thus, the membership function of the set X is:

$$\mu_A : X \rightarrow [0, 1] \quad (2.27)$$

We can distinguish three cases here:

- (a) $\mu_A(x) = 1$ —means full membership in the fuzzy set A
- (b) $\mu_A(x) = 0$ —means the lack of membership in the fuzzy set A
- (c) $0 < \mu_A(x) < 1$ —means a partial membership in the fuzzy set A .

A fuzzy set A is contained in the fuzzy set B only when $\mu_A(x) < \mu_B(x)$ for each $x \in X$, and the fuzzy set A equals the fuzzy set B only when $\mu_A(x) = \mu_B(x)$. The complement of the set A is a fuzzy set $\bar{A}$ with a membership function $\mu_{\bar{A}} = 1 - \mu_A$.

Although the inference based on the fuzzy set theory and multi-valued logic is more complex and less intuitive, thanks to widely available computer tools supporting the process of the fuzzy inference it is becoming more common (Klir and Yuan 1995).

(C) Non-standard fuzzy sets theories

A further generalization of the sets theory are non-standard fuzzy sets. These include, inter alia, fuzzy sets of type 2, for which the degrees of membership are also fuzzy sets (Mendel 2001). In this case, the membership function is expressed by:

$$\mu_A : X \rightarrow [0, 1]^{[0,1]} \quad (2.28)$$

A simpler variant of the above sets are interval-valued fuzzy sets, in which for every x a membership function μ_A has values in the interval $[0, 1]$.

2.2.2.2 Monotonic Measures

There is a set X and a non-empty family of sets C which are subsets of X and containing the empty set $\emptyset$ and the set X . A regular monotonic measure g on $\langle X, C \rangle$ is function

$$g : C \rightarrow [0, 1] \quad (2.29)$$

satisfying the following conditions:

1. $g(\emptyset) = 0$ and $g(X) = 1$ (boundary conditions)
2. for each $A, B \in C$, if $A \subseteq B$, then $g(A) \leq g(B)$ (monotonicity)
3. for each increasing sequence $A_1 \subseteq A_2 \subseteq \dots$ there is:

$$\text{if } \bigcup_{i=1}^{\infty} A_i \in C, \text{ then } \lim_{i \rightarrow \infty} g(A_i) = g\left(\bigcup_{i=1}^{\infty} A_i\right) \quad (2.30)$$

bottom-up continuity condition

4. for each decreasing sequence $A_1 \supseteq A_2 \supseteq \dots$ there is:

$$\text{if } \bigcap_{i=1}^{\infty} A_i \in C, \text{ then } \lim_{i \rightarrow \infty} g(A_i) = g\left(\bigcap_{i=1}^{\infty} A_i\right) \quad (2.31)$$

top-down continuity condition.

If we assume that $A, B \in C$ and $A \cap B = \emptyset$, in the theory of monotone measures, the following situations are possible:

1. $g(A \cup B) \geq g(A) + g(B)$ —superadditivity, or interaction (reinforcement) of A and B in relation to the assessed volume,
2. $g(A \cup B) = g(A) + g(B)$ —additivity, i.e. no dependence on A and B in relation to the assessed volume,
3. $g(A \cup B) \leq g(A) + g(B)$ —subadditivity, or incompatibility (weakening) of A and B in relation to the assessed volume.

(A) Additive measures—the “numeric” probability

Given a sample space $S = \{A_i\}$, the probabilities assigned to events A_i must satisfy these requirements (axioms of probability):

- (1) The probability of any event A_i must be nonnegative, e.g., $p(A_i) \geq 0$ for each i .
- (2) The probability of the entire sample space S must be normed to 1, i.e., $p(S) = 1$.
- (3) For a countable collection of mutually exclusive events A_i , the probability of the union A_i is equal to the sum of the probabilities of A_i , i.e., $P(A_1 \cup A_2) = P(A_1) + P(A_2)$.

There are three ways to assign probabilities to events: classical approach, relative-frequency approach, subjective approach.

- Axiomatic approach. If an experiment has n simple outcomes, then each outcome is assumed to have an equal probability of occurrence. This method would assign a probability of $1/n$ to each outcome.
- Frequency approach. Probabilities are assigned on the basis of experimental or historical data. If A is an event of interest, and assume that we have performed the same experiment n times so n is the number of times A could have occurred. Let n_A be the number of times that A did occur. Then, for large n , the ratio n_A/n may be taken as a reasonable approximation for $p(A)$.
- Subjective approach. In this approach, we define probability as the degree of belief that we hold in the occurrence of an event. Thus, judgment is used as the basis for assigning probabilities. The use of the subjective approach is usually limited to experiments that are unrepeatable.

The probability theory is a classic tool in studying uncertainty. Applying this theory leads to assumptions, such as that the rate of uncertainty should be measurable (using simple methods) and have a numerical rating. Another assumption used in the studies of uncertainty is the independence of the system components. Uncertainty and uncertain information are also modelled in this case by a probability distribution. For a finite set X of mutually exclusive alternatives, a probability distribution function for each $x \in X$ is

$$p(x) \in [0, 1] \quad \sum_{x \in X} p(x) = 1 \quad (2.32)$$

(B) Non-additive measures

A characteristic of non-additive measures is that the probability of the sum of mutually exclusive (independent) events does need not to equal probability of these events. This reflects a subjective assessment of probability by a decision-maker, which is not necessarily an objective probability. This condition is fulfilled by measures based on the possibility theory and the imprecise theory of probabilities.

(a) The possibility theory

The concept of *possibility and necessity* is the oldest and most fundamental concept of measures, derived from the ideas of Aristotle. However, the theoretical basis for this concept was developed by Zadeh (1978) in the 1970s. It is assumed that there is a set of mutually exclusive alternatives X . The basic information that we can

obtain on the set X (based on different types of tests) is the information that certain alternatives from a set X are impossible. After rejecting impossible alternatives, we obtain a set of possible alternatives E , which is a subset of X . The characteristic function of the set E (also known as the basic function of possibility) is:

$$r_E(x) = \begin{cases} 1 & \text{for } x \in E \\ 0 & \text{for } x \notin E \end{cases} \quad (2.33)$$

A function of possibility defined on a power set $P(X)$ is given by the formula

$$Pos_E(A) = \max_{x \in A} r_E(x) \text{ for each } A \in P(X) \quad (2.34)$$

A real alternative may belong to a set A if A contains at least one element of the set E . Functions of necessity can be formulated as follows:

$$Nec_E(A) = 1 - Pos_E(\bar{A}) \text{ for each } A \in P(X) \quad (2.35)$$

The real alternative is necessary in A only when it is not possible that it is in a completion of A . An uncertainty measure of a finite set of possible alternatives E is Hartley's measure expressed by the formula:

$$H(Pos_E) = \log_2 |E| \quad (2.36)$$

(b) The theory of imprecise probabilities

The theory of imprecise probabilities is used for experimental data burdened with uncertainty, for which it is difficult or even impossible to calculate the probability characteristics. A characteristic of all imprecise probabilities is that the data can be described by means of the low and high probability functions ($\underline{g}$ i $\bar{g}$). Functions $\underline{g}$ i $\bar{g}$ are regular monotonic measures and they fulfil the following conditions (Utkin 2004; Walley 1991):

$$\sum_{x \in X} \underline{g}(\{x\}) \leq 1, \quad \sum_{x \in X} \bar{g}(\{x\}) \geq 1 \quad (2.37)$$

The upper probability is a subadditive measure, and the lower probability is a superadditive measure. The classic probability measure is a special case of imprecise probabilities, for which lower and upper probabilities are equal.

2.3 Imperfect Knowledge Based Concept of Risk

2.3.1 Defining Risk

The concept of risk is very broad and covers many areas of human activity, and therefore has a social character. In the common sense, the risk is understood as a situation resulting in exposure to potential danger. Civil law defines the risk as “the danger of causing harm to the injured”. In the applied sciences, at the beginning of the 20th century, it was assumed that the risk is objectively dependent on subjective uncertainty, and a little later F. H. Knight (1921) published the theory of uncertainty, dividing the uncertainty into measurable (i.e. risk) and non-measurable (i.e. uncertainty *sensu stricto*). Based on these assumptions in the following years, many concepts of risk and their modifications were created, and successfully used to model risk for decision-making in particular areas of human activity, especially in business area.

An interesting summary in the search for a universal definition of risk is the work of Aven (2012), in which a critical review of the risk literature was made, and on this basis the classification of risk definitions into nine groups was proposed. Some of these definitions are only of historical significance, so they will be omitted in further considerations, while those that are currently of fundamental importance, according to the author, will be discussed. They were divided into three classes and characterized below (Bukowski 2015).

(a) Risk as expected value of a possible result.

This is historically the oldest quantitative approach to risk, attributed to mathematician de Moivre (1738), and still widely used as a part of financial analysis, as well as by making decisions using the so-called decision trees. In this approach, the measure of risk is the product of the occurrence probability of a given event and the financial consequences of this event. This class may also include the concept of Adams (1995), according to which the risk can be described by the product of the occurrence probability of a certain event and its utility (usefulness if it occurs).

(b) Risk as a combination of the effects of a certain scenario and the likelihood of this scenario's occurrence.

In this group, many risk assessment concepts can be located, but the most universal one is the proposal of Kaplan and Garrick (1981), who define the risk as the triplet (s_i, p_i, c_i) , where s_i is the i -th unwanted disruption scenario, p_i is the uncertainty metric (probability) of this scenario, and c_i is the severity metric (consequence) of the i -th scenario, for $i = 1, 2, 3, \dots, n$. This group includes also the definition recommended by the EN-N-18 002 standard, according to which the risk is a combination of the occurrence frequency or probability of a specific event causing the threat, and consequences related to this event.

(c) Risk as a result of uncertainty in achieving the assumed goals.

This is the most general approach, recommended by the ISO 31000 standard in the 2009 version. It is based on the idea already proposed by Hardy (1923), who under the concept of risk understood the uncertainty about the costs, losses and damage that may occur in the future. This approach allows to clarify the “operational” concept of risk, depending on the specificity of the problem and the perspective from which it is considered. The class (c) could also include new trends in risk research, represented for example by Committee on Foundations of Risk Analysis, and presented in SRA Glossary (2015). This perspective includes additional judgment of the strength of the background knowledge which supports the risk assessment procedures.

Based on the above considerations and taking into account the possibility of uncertainty modelling, it is proposed to provide a universal approach to risk, from a qualitative and quantitative perspective as follows:

Qualitative definition:

Risk is the potential of gaining or losing something of value (such as physical health, social status, or financial wealth) resulting as an outcome from a given activity (planned or not planned) taken in spite of uncertainty.

Quantitative definition (based on Aven 2012):

Risk description for a given *activity* A can be represented by the triplet (C, U, K) , where C is some specified *consequences*, U the *uncertainty* associated with C , and K the *background knowledge* that supports C and U (which includes a judgment of the strength of this knowledge).

We understand the basic terms of the quantitative definition as follows:

Activity (A)—an intentionally designed and implemented action. We divide activities into operations, tasks and decisions.

Consequences (C)—the effects of an activity with respect to the values defined (such as human life and health, environment and economic assets), covering the totality of states, events, barriers and outcomes, and often seen in relation to some reference values (planned values, objectives, etc.).

Uncertainty (U)—a situation of having imperfect knowledge about the true value of a quantity or the future consequences of an activity, scenario or event.

Background knowledge (K)—the ability to evaluate available information and understand reality in accordance with the current state of knowledge, including a judgment of the strength of this knowledge.

The risk description model can be shown in the following form:

$$R(A) = (C, U, K) \quad (2.38)$$

where: $A = \{a_i\}$; $C = \{c_i\}$; $U = \{u_i\}$; $K = \{k_i\}$ for $i = 1, 2, 3, \dots, n$

In this approach, all three above distinguished classes of risk definitions—(a), (b) and (c)—can be described by one, universal model expressed by formula (2.38). For example in the case of the traditional approach (class a), the set of consequences

will be described in the language of classical sets theory, and the set of uncertainty measures will be estimated on the basis of probability theory and mathematical statistics. In the most general case, the set of consequences will be described in the language of fuzzy sets theory, and the set of uncertainty measures will be estimated on the basis of possibility theory (e.g. possibility and necessity functions).

2.3.2 *The Role of Background Knowledge in Risk Analysis*

Based on the risk description model (1) we will discuss the role of background knowledge in risk analysis. We understand the term *risk analysis* in broad perspective, as a systematic process to comprehend the nature of risk and to express the risk, with the available knowledge. It includes risk assessment, risk characterization, risk communication, risk evaluation, risk framing, risk governance, and risk management, as well as policy relating to risk, in the context of risks to individuals, the public, organizations, and to society. Therefore, the comprehensive risk analysis process consists of the following stages:

- *Risk assessment*—systematic process to comprehend the nature of risk, express and evaluate risk, with the available knowledge.
- *Risk characterization*—a qualitative and/or quantitative description of the risk; i.e., a structured statement of risk usually containing the following elements: risk sources, causes, events, consequences, uncertainty measurements and the knowledge that the judgments are based on.
- *Risk communication*—exchange or sharing of risk-related data, information and knowledge between and among different target groups (such as regulators, stakeholders, consumers, media, general public).
- *Risk evaluation*—process of comparing the result of risk analysis against risk (and often benefit) criteria to determine the significance and acceptability of the risk.
- *Risk framing*—the initial assessment of a risk problem, clarifying issues and defining the scope of subsequent work.
- *Risk governance*—the application of governance principles to the identification, assessment, management and communication of risk. Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented.
- *Risk management*—activities to handle risk such as prevention, mitigation, adaptation or sharing. It often includes trade-offs between costs and benefits of risk reduction and choice of a level of tolerable risk.

Rumsfeld (2011), Former US Defence Secretary, commented at the Pentagon news briefing on 12 February 2002: “Reports that say that something hasn’t happened are always interesting to me, because as we know, there are known knowns; there are things we know. We also know there are known unknowns; that is to say

we know there are some things we do not know. But there are also unknown unknowns—the ones we don’t know we don’t know.” This sentence expresses simply and clearly the differences between the explicit knowledge (existing, available and accessible) and the tacit knowledge (hidden meta-knowledge, our knowledge about knowledge). Assuming the two-dimensionality of the knowledge concept, we should also include a fourth case, namely “unknown knowns”, i.e. existing knowledge which we are not aware of.

Figure 2.9 presents a two-dimensional knowledge matrix built on the basis of these four possible combinations. In the top right quadrant I lies *Certainty* (‘known knowns’), where the extent of what is known is fully understood. This is an area of no real risk, including variability subjected to known rules, such as well-described seasonal changes and long-term trends. Below there is the area III of *Unconscious Uncertainty* (‘unknown knowns’), representing a hidden knowledge to decision makers. Usually this is due to the so-called organizational amnesia, which is the result of incorrect knowledge management in a given company (e.g. lack of knowledge culture). The top left corner II belongs to *Conscious Uncertainty* (‘known unknowns’), where we are aware of a knowledge imperfection. This is an area of typical risk, including variability subjected to random rules. And quadrant IV in the bottom left section represents *Deep Uncertainty* (‘unknown unknowns’), with pure ignorance of the situation faced.

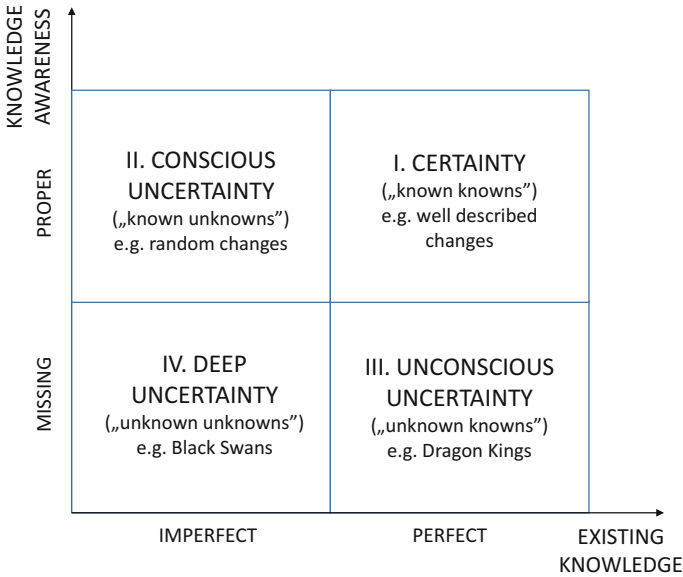


Fig. 2.9 Knowledge matrix

Each of these zones requires a different approach:

- I. *Certainty*—complete perfect knowledge. The knowledge should be exploited, making full use of known facts to take well-founded decisions and activities. The basic tools used in this area are operational research methods and analytical models.
- II. *Conscious Uncertainty*—strong imperfect knowledge. Areas of ‘known unknowns’ should be carefully explored, seeking to understand the implications of uncertainty or deficiency of knowledge. The basic tools used in this area are stochastic and statistics.
- III. *Unconscious Uncertainty*—weak imperfect knowledge. The organizational amnesia needs to be exposed, e.g. through a facilitated process, to unlock the knowledge that exists and to use it effectively. The area includes so-called ‘Dragon Kings’.
- IV. *Deep Uncertainty*—lack of knowledge. Ignorance can only be tackled through experiment or by gaining experience, growing in both knowledge and its awareness, to reduce the size of this area, sometimes called ‘Black Swan’.

Dragon king is a metaphor for an event that is both extremely large in size or impact (a ‘king’) and belongs to unique origins (a ‘dragon’) relative to other events from the same system. Dragon king events are generated by different phenomena such as positive feedbacks, tipping points, bifurcations, and phase transitions, that tend to occur in complex, nonlinear systems, and serve to amplify these events to extreme levels. By understanding and monitoring the dynamics of these systems, some predictability of such events may be obtained.

The theory has been developed by Sornette (2009), who hypothesizes that many of the crises situations that we face are in fact dragon kings rather than black swans; i.e., they may be predictable to some degree. The dragon kings theory urges that special attention should be given to the study of the system dynamic and monitoring of extremes. From a practical viewpoint, such extremes are interesting because they may reveal underlying, often hidden, organizing behavioural principles. This means we need to study extreme systems behaviour, but not forget that significant uncertainty will almost always be present, and should be rigorously considered in decisions regarding risk management and design. The theory of dragon kings is related to concepts such as: black swan theory, outliers, complex systems, nonlinear dynamics, power laws, extreme value theory, prediction, extreme risks, risk management, etc.

Black swan can be considered as a metaphor for an event that is surprising (to the observer), has a major effect, and, after being observed, is rationalized in hindsight. The theory of black swans is epistemological, relating to the limited knowledge and understanding of the observer. The term was introduced and popularized by Taleb (2010) and has been associated with concepts such as heavy tails, non-linear payoffs, model error, and ‘unknowable unknown’ event terminology (popularized by Donald Rumsfeld). However, claiming that extreme events are—in general—unpredictable may also lead to a lack of accountability in risk management roles.

In practice, in a wide range of physical systems the extreme events are predictable to some degree. To achieve it we need to have a sufficiently deep understanding of the structure and dynamics of the system under consideration, and the ability to monitor it. Therefore, this is exactly the domain of the dragon kings. It is widely known that many phenomena in both the natural and social sciences can be described by power law statistics (so-called Pareto distribution). Furthermore, a broad range of distributions (e.g. the Frechet class) have tails that are asymptotically close to the power law distribution. It means, when dealing with crises and extremes, power law tails are the typical case. The unique property of power laws is that they are scale-invariant, self-similar and fractal. This property implies that all events are generated by the same mechanism, and thus there will be no distinct precursors by which the largest events may be predicted. A conceptual framework for events of this type is so-called self-organized criticality. Such concepts are compatible with the theory of the black swan. In a variety of studies it has been found that, despite the fact that a power law models the tail of the empirical distribution well, the largest events are much bigger than it would appear from the model. Such events are interpreted as dragon kings because they indicate a departure from the generic process underlying the power law. Physically, dragon kings may be associated with the system or process changes, bifurcations, and tipping points of complex systems in states far from equilibrium. Positive feedback is also a mechanism that can induce dragon kings (e.g. physical resonance or herd behaviour).

Dragon kings are also caused by attractor bubbling in nonlinear complex systems. Attractor bubbling is a generic behaviour appearing for example in networks of coupled oscillators where the system typically orbits in an invariant manifold with a chaotic attractor where the peak trajectories are low, but is intermittently pushed by noise into a region where the peak trajectories are large. It is claimed that such models can describe many real phenomena in complex systems such as earthquakes, brain activity, etc. (e.g. a model of geological faults and their earthquake dynamics, produced a similar distribution) (e.g. Show et al. 1992).

In some cases dragon kings are created as a result of system control or external intervention. For instance, forest fires are a natural occurrence in areas with a dry climate. If the preventive activity of man will avoid fires for a long time, then this leads in the absence of fires, to dead wood accumulates. Once this accumulation reaches a critical point, and a fire starts, the fire becomes so large that it cannot be controlled, and this singular event could be considered to be a dragon king. Other policies, such as doing nothing (allowing for small fires to occur naturally), or performing strategic controlled burning, would avoid enormous fires by allowing for frequent small ones.

The background knowledge which is necessary to conduct risk analysis is multidimensional and concerns, among others, different risk factors that affect each activity, namely:

- Novelty—uniqueness, involving at least some elements that have not been done before.

- Synergy—complexity of various kinds, including technical, commercial, interfaces or relational, causing difficulties in assessing the behaviour of the entire complex system.
- Unpredictability—assumptions and constraints about the future, both explicit (open) and implicit (hidden), which may be wrong.
- Change of goals over time—objectives, defining the measures by which system will be determined, are usually fixed and sometimes conflicting.
- Human factors—people (clients and customers, suppliers and subcontractors) are unpredictable to some extent.
- Stakeholder requirements—expectations and objectives, which can be varying, overlapping and sometimes conflicting.
- Environment—including both the internal organisational environment and the external environment where changes beyond control can occur.

Because, in practice, it is impossible to know all these risk factors when making complex decisions, so in reality almost always we deal with making decisions based on imperfect knowledge. Therefore, the awareness of the degree of this knowledge imperfection is particularly important.

2.3.3 Risk Types and Its Metrics

Based on the risk description model proposed in Sect. 2.3.1 in the form (2.38) we can define the risk metric for a system as following:

Risk metric is the triplet (C', U', K) , where C' is a measure of some consequences C for a specific value V resulting as an outcome from a given activity A (e.g. positive or negative impact), U' represents a measure of uncertainty U associated with C' (e.g. probability or possibility), and K is the background knowledge that supports evaluation of C' and U' (including a judgment of the strength of this knowledge).

The above definition is sufficiently universal to cover all types of risk, but for a quantitative assessment for a specific case is too general. Therefore, to propose specific quantitative measures for particular types of risk, three basic groups of risks should be distinguished, namely:

- I. Opportunity related risks—covering the risk of lost and missed chances
- II. Hazard related risks—including all risks in a safety context
- III. Threat related risks—concerning risks of detriment, namely:
 - a. Economic risk—the potential of losing something of value such as financial wealth, e.g. financial, commercial and price risks.
 - b. Technical risk (operational risk)—risk in context of operation system unavailability, e.g. potential for realization of unwanted scenario leading to a disruptive event with possibility of negative consequences.

In the following, we will discuss this basic groups of risks and propose quantitative risk measures for them.

Group I—opportunity related risks

Opportunities can emerge both, from within the organization as well as beyond the organization. The main potential sources of opportunity inside the organization are following:

- Supply infrastructure—innovation in the area of how value is created and delivered to the market, can be a source of opportunity. The company structures itself, partners with their entities, as well as operates to deliver its products and services should be examined for opportunities. Usually an innovation is possible at many of the links along the whole supply chain or network.
- Product and service—the search for opportunities and innovation can also concentrate on new products and services, or modifications to existing products and services. Increasingly, customers are expecting these types of innovations, and organization which can identify and deliver on these expectations often achieves great incomes.
- Process and technology—process improvement can lead to faster, better, and less expensive products. New and innovative technology provides another source of opportunity by allowing companies to execute strategy quickly, thereby making time a source of competitive advantage.
- Markets—new markets often create opportunities to source products differently or tap into new consumer groups.

Sources of opportunity outside the organization:

- Clients and customers—sensitivity to clients and customer needs can open views on opportunities. Companies that focus on shifts in customer behaviour and their trends can anticipate changes, and through innovation, meet this needs before their competition does.
- Complementors and competitors—being sensitive to the opportunities owned by the competition can provide important information. Also, developing sensitivity how competitors avoid some risks can yield opportunity.
- Emerging technologies—new technologies and scientific developments, even when not apparently related to one particular industry, can also be a source of opportunity. For instance, the Internet revolutionized commerce business when supermarkets began offering online shopping and delivery.
- Political, legal and social forces—opportunities can be found in the political, legal, and social area in which business is conducted. For example, the increasing concern over climate change and negative human impact on the environment has led many companies to develop “green products” to meet both consumer demand and increased legislative pressures.

The problem of using risk opportunities is closely related to the concept of risk appetite. Risk appetite is generally defined as amount and type of risk, that an

individual or an organisation is willing to take on risky activities in pursuit of values or interests. After reaching the threshold of risk appetite, we can take action to restore the level of exposure back to the acceptable range, thus balancing the risk exposure with the risk appetite. Risk appetite can also be described as risk tolerance, supported by risk management. A company's risk appetite is strongly influenced by its culture and flexibility. Each major opportunity and risk must usually be examined to evaluate whether it falls within tolerable limits. To assess and determine risk appetite, it can be useful to begin with asking the following four questions (RIMS 2011):

- Where should the organization allocate its limited time and resources to maximize opportunity and minimize risk exposure?
- Which opportunities and what level of risk exposure require immediate action, and why? Have other issues such as alternative opportunities, market reaction, and resource allocation been evaluated? Are reputation, regulatory interference, and impact on credit rating being included?
- What types of opportunities and what level of risk require a formal response strategy, and why? What happens if the type or level is changing (higher or lower)?
- What opportunities has the organization missed, and what risks affected the organization in the past? How were they handled and who managed them?

These issues should be based on risk tolerances as well as levels of risk exposure predetermined for the organization and based on authority and approved by the board.

A variety of factors influence an organization's level of risk appetite and its ability to accept more risk. These include: willingness to risk, organizational size, financial health, reputation, experience, and agility (based on RIMS 2011):

- *Willingness to risk*—this can often be attributed to their leadership or structure—the propensity towards risk is often in the tradition of the organization. Companies with an increased willingness to risk may have a higher tolerance than their more cautious counterparts.
- *Organizational size*—the size of an organization can influence risk appetite. Larger more diversified companies are exposed to a wide variety of risks. They are often comfortable with this because risks and exposure are spread across the business and, thus, any one event is likely to have a smaller impact. This also holds true for the size of the investment compared to the overall portfolio.
- *Financial health*—a healthy firm is often in a strong position to take on more risk, because it can withstand potential losses more easily than a less healthy one. The higher risk appetite due to financial health can encourage companies to take advantage of innovation opportunities which another company might not be able to take.
- *Reputation*—corporations with strong reputations often have a higher risk appetite because their stakeholders and shareholders usually have more confidence that the company will take risks without putting the business at stake.

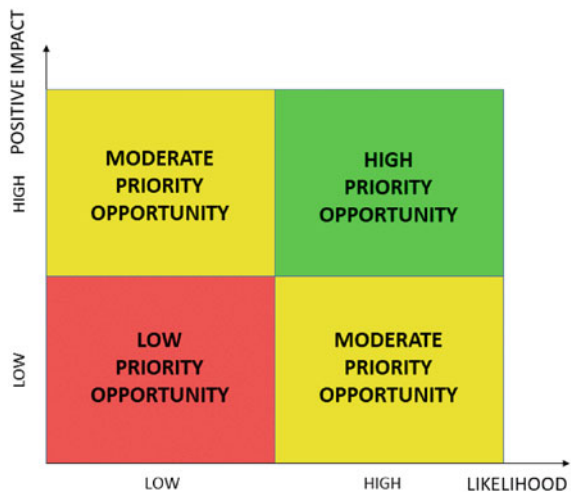
However, this is not the case for businesses based on trust where product safety is in central focus.

- *Experience*—availability of historical data about dealing with specific risks often helps organizations to improve risk management and responses to opportunities over time. A company with significant global experience is often better able to analyse, capitalize on, and react to opportunities and risks in its international operations than a new one.
- *Agility*—an agile company is one that predicts risk well and can respond quickly and effectively to risks and opportunities. These organizations can measure risk early and therefore plan for it. Establishing protocols for events ranging from supply chain disruptions to inclement weather can help a company withstand the impact if risks materialize, and take advantage of the chances if this happens.

In order to quantify the opportunity related risk, we can use modified risk matrices, in which the likelihood of a favourable chance is on the X axis and the positive impact of this chance on the Y axis. Figure 2.10 shows an example of an opportunity related risk matrix for situations with a weak background knowledge. In these cases it is advisable to limit the resolution in the assessment of risk parameters to two classes—low and high—which gives us four possible combinations for the priority opportunity assessment, and three option (low, moderate and high priority opportunity). If we have strong background knowledge, the resolution of risk parameters should be higher. An example of an opportunity related risk matrix for situations with a strong background knowledge shows Fig. 2.11. In this case, we have five classes for likelihood (L), namely:

- very low—very unlikely occurrence (e.g. has not happened before),
- low—slight, rarely occurs,
- moderate—feasible and possible, but not common,

Fig. 2.10 Opportunity related risk matrix for weak background knowledge



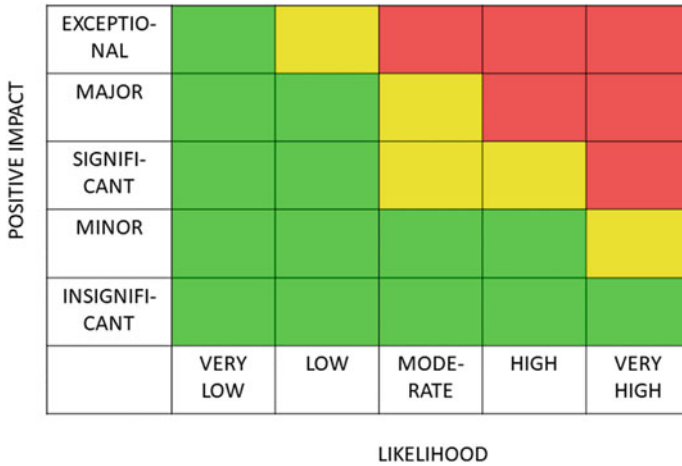


Fig. 2.11 Opportunity related risk matrix for strong background knowledge

- high—likely, has happened before and can again,
- very high—high probable, occurs frequently,

and five classes for positive impact (*PI*):

- insignificant—no noticeable relevant effect,
- minor—only little effect available,
- significant—moderate improvement observable,
- major—important, substantial and relevant positive effect,
- exceptional—crucial, essential or vital positive effect.

As a result, we get 25 combinations, which can be divided into three or more priority opportunity classes. In Fig. 2.10 we have three classes, namely: low priority opportunity (without background), moderate priority opportunity (dotted background), and high priority opportunity (chequered background).

Group II—hazard related risks

The context of hazard is usually understood broadly and concerns both the human factor (often called occupational risk) and the environmental safety. We will understand the term *hazard* as a risk source where the potential consequences relate to safety application (e.g. harm). In case where hazard is focused on loss of human lives, the *FAR* (Fatal Accident Rate) measure is used to describe the level of risk. The *FAR* is defined as the expected value of life loss per 100 million h of exposure to risk source. This time period corresponded approximately to the time of 1000 person present at their workplace through a full life span.

A more practical measures are *PLL* (Potential Loss of Life) and *AIR* (Average Individual Risk). *PLL* is defined as the expected number of fatalities over a year, and can be express with the formula:

$$PLL = n \times t \times FAR / 10^8 \quad (2.39)$$

where:

n number of person exposed to a hazard for t hours per year.

AIR is the average probability of dying in an accident for n person, so:

$$AIR = PLL / n \quad (2.40)$$

An alternative way of describing the risk associated with loss of lives is the F–N curve (Frequency–Number of Fatalities). An F–N curve shows the frequency of accident events with at least N fatalities, where the axes are usually logarithmic. It describes the risk related to large-scale accidents and is thus especially useful for characterising societal risks. Various normalisations may be used depending on the application involved. For example, in a transportation context, we are primarily concerned with the expected number of fatalities and injuries per kilometre and year (Aven 2015). We can also use a risk matrix as the tool for describing hazard-related risk.

There are many qualitative methods for occupational risk assessment (e.g. workplace risk analysis). One of the most popular is the Risk Score methodology in which the risk indicator is calculated as the product of: the event occurrence probability (P), the size of exposure to hazard (E), and the severity of potential outcome of such an event. Parameter (P) may take seven possible values from 0.1, in case of events that are only theoretically possible, to 10 for highly probable events. There are six values from 0.5 (exposure once per year) to 10 (continuous exposure). The severity of potential outcome of events is determined in two ways—regarding the damage to human’s health or with regard to the possible resource losses. Parameter (S) may have values from 1, when there are only minor injuries possible, to 100, when there is a real possibility of fatal accidents. The formula to calculate the risk indicator is following:

$$R_{RS} = P \cdot E \cdot S \quad (2.41)$$

where:

R_{RS} risk indicator in the Risk Score method,

E exposure to hazard,

P probability of hazard occurrence,

S severity of potential outcome of the risks.

Table 2.5 shows an example of risk categorizing based on this methodology.

The standard EN-1050 entitled “Safety of machinery—Principles of risk assessment” gives detailed rules for the safety risk evaluation together with numerous specific instances (e.g. a list of over 100 different examples of threats, emergency situations and threatening events).

There are also many other methods known and used in individual cases, such as:

Table 2.5 Risk categorizing matrix for the risk score methodology

No.	Risk indicator value	Risk category
1	$R_{RS} < 2.5$	Negligible
2	$1.5 < R_{RS} \leq 48$	Acceptable
3	$48 < R_{RS} \leq 270$	Average
4	$270 < R_{RS} \leq 1440$	Serious
5	$R_{RS} > 1440$	Unacceptable

- CCA—Cause and Consequences Analysis,
- CHL—Check List Analysis,
- DIN 19,250—Risk Graph Methodology,
- HRA—Human Reliability Assessment,
- PHA—Preliminary Hazard Analysis,
- PSA—Process Safety Analysis.
- and methods included in standards e.g.: MIL STD 882, BS 8800.

Because a rich literature is available on this subject, we will not be devoting them more place in this work.

Group III—threat-related risks

This group of risks concerns the possibility of a detrimental effect connected with some tangible, material losses as well as damage, and is divided into two subgroups, namely: economic risk and operational risk.

A. *In the area of the economic risk we can distinguish:*

- *Financial risks*—the probability that an actual return on an investment will be lower than the expected return. Financial risk is divided into the following categories: Basic risk, Capital risk, Country risk, Default risk, Delivery risk, Economic risk, Exchange rate risk, Interest rate risk, Liquidity risk, Solvency risk, Operations risk, Payment system risk, Political risk, Refinancing risk, Reinvestment risk, Settlement risk, Sovereign risk, and Underwriting risk.
- *Insurance risks*—a situation where the probability of a variable (such as burning down of a building) is known but when a mode of occurrence or the actual value of the occurrence (whether the fire will occur at a particular property) is not. A risk is not an uncertainty (where neither the probability nor the mode of occurrence is known), a peril (cause of loss), or a hazard (something that makes the occurrence of a peril more likely or more severe).
- *Trading risks*—the probability of a loss or drop in value. Trading risk is divided into two general categories: (1) Systemic risk affects all securities in the same class and is linked to the overall capital-market system and therefore cannot be eliminated by diversification. Also called market risk. (2) Non-systemic risk is any risk that is not market-related or is not systemic. Also called nonmarket risk, extra-market risk, or unsystemic risk.

The above-mentioned risk types belong to the business risk area and are regulated by international standards. The most important standards in force, both in production corporations and in services (including banking), are following:

- Cadbury Report (1992)—Financial Aspects of Corporate Governance,
- Turnbull Report (1998)—Combined Code of Corporate Governance,
- KonTraG (1998)—Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (modification of the Commercial Code),
- Sarbanes-Oxley Act (2002/2004)—Risk Management Reports,
- COSO I (1992)—Integral Control—Integrated Framework (an internal control standard),
- COSO II (2004)—Enterprise Risk Management (an integrated risk management system),
- CAS (2003)—risk management process model in 7 steps,
- FERMA (2003)—organization of the risk management process.

In order to quantify the economic risk, different measures are used, but the most common are:

Expected Value (EV), Standard Deviation (SD), Value at Risk (VaR), and Expected Shortfall (ES). All the risk measures have strengths and weaknesses, since no single measure can capture all the complex elements of this type of risks. Expected value and standard deviation are typical probabilistic measures and can be easily determined using statistical methods (if we have access to representative statistical data). However, value at risk and expected shortfall are typical risk assessment metrics for economic applications.

VaR is defined as the maximum loss on a certain investment over a given period of time, with a certain probability (e.g. 95%). Although this definition seems to be completely unambiguous, there are as many as three different ways to measure the VaR value. The reason for this is that VaR is subadditive for elliptical distributions, such as the normal distribution, whereas it is not subadditive for non-elliptical distributions. The non-subadditivity of VaR can occur when:

- (a) variable X (e.g. assets in portfolios) have very skewed loss distributions; or
- (b) the loss distributions of X are smooth and symmetric, but their dependency structure or copula is highly asymmetric; or
- (c) underlying risk factors are independent but very heavy-tailed.

The lack of subadditivity for VaR is more of a concern for credit risk than for market risk, where an elliptical distribution may be a reasonable approximate model for various kinds of risk-factor data (Basel 2008).

Expected Shortfall (ES) is a loss measure estimate given a loss range in the tail of the loss distribution, while VaR is a loss measure estimated given a particular point in the tail of the loss distribution. ES is coherent, making capital allocation and internal limit setting consistent with the overall portfolio measure of risk. Furthermore, ES is a more stable measure than VaR with respect to allocating the overall portfolio capital to individual facilities. However, ES does not lend itself to

easy interpretation and does not afford a clear link to a bank's desired target rating. A newer class of risk measures, known as spectral and distorted risk measures (Basel 2008), allow for different weights to be assigned to the quantiles of a loss distribution, rather than assuming equal weights for all observations, as is the case for ES.

Currently, there is a very extensive literature on the methods of assessing and measuring the economic risk to which we refer interested readers.

B. *In the area of the technical risk we can distinguish a lot of the well-known methods, such as:*

- HAZOP—Hazard and Operability Studies according to IEC 60300-3-9,
- FMEA—Failure Mode and Effects Analysis according to IEC 812,
- FMEA—Fault Mode and Effects Analysis according to IEC 50(191),
- FMECA—Failure Mode, Effects and Criticality Analysis according to IEC 812,
- FMECA—Fault Mode, Effects and Criticality Analysis according to IEC 50 (191),
- FTA—Fault Tree Analysis according to IEC 1025,
- ETA—Event Tree Analysis according to IEC 60300-3-9,
- PHA—Preliminary Hazard Analysis according to IEC 60300-3-9.

Since these methods are widely used in the original versions as well as in many modifications, they will not be discussed in this paper. However, we will present an Process Failure Mode and Effects Analysis model, based on a concept of ISO/TS 16949:2009 titled FMEA AIAG 4th edition. This method seems to be particularly suitable for the case of an operational risk assessment.

Process Failure Mode and Effects Analysis (PFMEA) is a methodical approach used for identifying risks related to process changes, and focused on potential process failures and their causes. The PFMEA initially identifies process functions, failure modes, their effects on the process and the effect on end user. The consequence of the effect is determined for each effect of failure. Then, causes and their mechanisms of the failure mode are identified. Based on the Appendix E of the AIAG, Potential Failure Mode and Effects Analysis (FMEA) (AIAG 2008), the basic concepts used in PFMEA are defined in the following way:

Function (FU)—the objective which the process is intended to do, to a given standard of performance or requirement. For Process FMEAs, this is the primary purpose of the delivering, manufacturing or assembly operation. There may be many functions for each operation.

Failure (FA)—the state or condition of inability to perform a required function.

Failure Cause (FC)—the specific reason for the failure. For PFMEAs, the cause is the process deficiency (or source of variation) that results in the failure mode; if a cause occurs, the corresponding failure mode occurs. There can be many causes for each failure mode.

Failure Mode (FM)—the manner in which the item or operation fails to meet or deliver the intended function and its requirements. Failure modes may include

failure to perform a function within defined limits, inadequate or poor performance of the function, intermittent performance of a function, and/or performing an unintended or undesired function. There may be many failure modes for each function.

Failure Effect (FE)—the consequence of the failure on the system or end user. For PFMEAs, usually we consider the effect of the failure at the delivering, manufacturing or assembly level, as well as at the system or end user. There can be more than one effect for each failure mode, but generally we use the most serious of the end effects for the analysis.

Process Controls (PC)—the methods or actions to reduce or eliminate the risk associated with each potential cause. Controls can be the methods to prevent or detect the cause during product development, or actions to detect a problem during service before it becomes disastrous. There can be many controls for each cause.

Prevention-related Process Controls (PPC)—the methods that describe how a cause, failure mode, or effect in the delivering, manufacturing or assembly process is prevented. They are intended to reduce the likelihood that the problem will occur, and are used as an input to the occurrence ranking.

Detection-related Process Controls (DPC)—the methods that describe how a failure mode or cause in the delivering, manufacturing or assembly process is detected. They are intended to increase the likelihood that the problem will be detected before the item is shipped from the manufacturing or assembly plant, and are used as an input to the detection ranking.

Corrective Actions (CA)—the tasks that can be performed to reduce or eliminate the risk associated with potential cause of failure. Corrective actions should consider the existing controls, the relative importance of the issue, and the cost and effectiveness of the recommended action. There can be many types of actions for each cause.

Ranking Numbers (RN)—usually integer numbers ranging from 1 to 10.

Severity (S)—a ranking number associated with the most serious effect for a given failure mode based on the criteria from a severity scale. It is a relative ranking within the scope of the specific PFMEA and is determined without regard to the likelihood of occurrence or detection.

Occurrence (O)—a ranking number associated with the likelihood that the failure mode and its associated cause will be present in the item being analysed. For PFMEAs the occurrence ranking considers the likelihood of occurrence during delivering or production process. It is based on the criteria from the corresponding occurrence scale. The occurrence ranking has a relative meaning rather than an absolute value and is determined without regard to the severity or likelihood of detection.

Detection (D)—a ranking number associated with the best control from the list of detection-type controls, based on the criteria from the detection scale. The detection ranking considers the likelihood of detection of the failure mode/cause, according to the defined criteria. Detection is a relative ranking within the scope of the specific PFMEA and is determined without regard to the severity or likelihood of occurrence.

Risk Priority Number (RPN)—is a numerical ranking (usually integer numbers ranging from 1 to 1000) of the risk of each potential failure mode/cause, made up of the three elements product: severity of the effect, likelihood of failure mode occurrence/cause, and likelihood of detection of the failure mode/cause.

The risk assessment is made by determining the value of the Risk Priority Number (RPN). Risk Priority Number is Severity S (Table 2.6) multiplies by Occurrence O (Table 2.7) and Detection D (Table 2.8):

$$RPN = S \times O \times D \quad (2.42)$$

RPN Target ($RPNT$) defines the boundary between acceptable and unacceptable risk, and will be fixed based on the Severity ranking for initiating action on failure mode or causes. The following $RPNT$ will be used during PFMEA unless otherwise specified by the customer:

$RPNT < 100$ for $S = (1-7)$,
 $RPNT < 36$ for $S = (8 \text{ or } 9)$,
 $RPNT < 10$ for $S = 10$.

Once the expert team have completed the initial identification of failure causes, failure modes and failure effects, as well as process controls, including rankings for severity, occurrence and detection, they have to decide if further efforts are needed

Table 2.6 PFMEA severity ranking (AIAG 2008)

S-Rank	Effect	Severity of effect on process
1	No effect	No discernible effect
2	Minor disruption	Slight inconvenience to process, operation or operator
3	Moderate disruption	A portion of the production run may have to be reworked in-station before it is processed
4	Moderate disruption	100% of the production run may have to be reworked in-station before it is processed
5		A portion of the production run may have to be reworked offline and accepted
6		100% of the product may have to be reworked offline and accepted
7	Significant disruption	A portion of the production may have to be scrapped. Deviation from the primary process including decreased line speed or added manpower
8	Major disruption	100% of product may have to be scrapped. Line shutdown or stop ship
9	Failure to meet safety and/or regulatory requirements	May endanger operator (machine or assembly) with warning
10		May endanger operator (machine or assembly) without warning

Table 2.7 PFMEA occurrence ranking (AIAG 2008)

O-Rank	Occurrence of cause (incidents per items)	Likelihood of failure
1	Eliminated through preventive control	Very low
2	1 in 1,000,000	Low
3	1 in 100,000	
4	1 in 10,000	Moderate
5	1 in 2000	
6	1 in 500	
7	1 in 100	High
8	1 in 50	
9	1 in 20	
10	1 in 10	Very high

Table 2.8 PFMEA detection ranking (AIAG 2008)

D-Rank	Opportunity for detection	Likelihood of detection
1	Detection not applicable; error prevention	Almost certain
2	Error detection and/or problem prevention	Very high
3	Problem detection at source	High
4	Problem detection post processing	Moderately high
5	Problem detection at source	Moderate
6	Problem detection post processing	Low
7	Problem detection at source	Very low
8	Problem detection post processing	Remote
9	Not likely to detect at any stage	Very remote
10	No detection opportunity	Almost impossible

to reduce the risk. The main focus of the expert team should be oriented towards failure modes with highest severity rankings. When the severity rank is 9 or 10, they must ensure that the risk is mitigated by process controls or recommended corrective actions. For failure modes with severity ranks 8 or below the expert team should consider causes having highest occurrence rank, and next detection ranking. If occurrence rate is greater than 8, then action(s) is initiated in order to reduce the likelihood of failure mode occurrence.

Recommended actions are as following (AIAG 2008):

- In general, prevention actions are preferable to detection actions. An example of this is the use of process design error proofing rather than random quality checks or associated inspection.
- The intent of any recommended action is to reduce rankings in the following order: Severity, Occurrence, and Detection.
- If *RPN* value is higher than the *RPNT*, then action is initiated to reduce the *RPN* value.

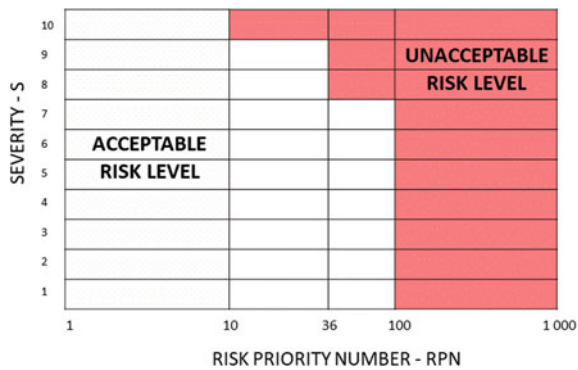


Fig. 2.12 Criterion for the interpretation of the RPN assessment results

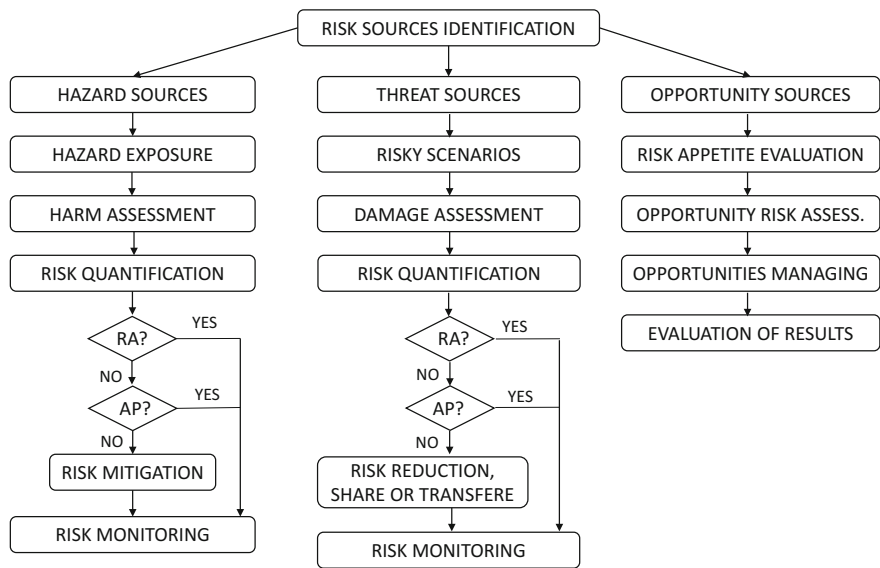


Fig. 2.13 Risk assessment algorithm for the three major risk sources

- If Occurrence rate is greater than 8, then action is initiated irrespective of *RPNT* in order to reduce the Occurrence rate.

Figure 2.12 shows the way of interpreting the results of the RPN assessment due to the severity *S* of a failure.

As a summary of this point, we propose a collective risk assessment algorithm for the three main sources of risk, which is presented in Fig. 2.13. Because logistics networks are primarily exposed to threats, and especially in the area of the operational risk, the problem of analysing this risk group will be discussed in more detail in the next section.

2.3.4 Modelling Operational Risk Based on the Imperfect Knowledge Concept

We propose a quantitative model for operational risk, which is based on the risk metric definition from the Sect. 2.3.3. As a measure of operational risk for a given risky scenario, we accept the triplet of attributes of this scenario, namely:

$$R(S_i) = (C'_i, P'_i, K'_i) \quad (2.43)$$

where:

- $R(S_i)$ risk measure for a risky scenario S_i ,
- C'_i consequence measure for a risky scenario S_i (e.g. severity of the scenario impact),
- P'_i uncertainty measure for a risky scenario S_i (e.g. likelihood of the scenario occurrence),
- K'_i knowledge measure for a risky scenario S_i (e.g. knowledge maturity level for the scenario and its attributes)

In practice, the first two attributes are considered together and presented in the form of so-called risk matrix. Simple examples of such matrices for opportunity related-risks are shown in Figs. 2.9 and 2.10. In the general case, for the construction of a risk matrix, we can use different types of measurement levels, often called scale of measure. *Scale of measure* is a classification that describes the nature of information within the values assigned to variables. The traditional classification with four levels of measurement was proposed by Stevens in 1946 (Kirch 2008), namely: nominal, ordinal, interval, and ratio, unifying both description, that is qualitative (with linguistic variables) and quantitative (with numeric variables). Chrisman (1998) introduced an expanded list of measurement levels to account for various measurements that do not fit to Stevens' original work. Measurements bound to a range and repeating, graded membership categories, as well as other types of measurement were leading to the introduction of six new levels of measurement, namely: gradation of membership (e.g. based on fuzzy set theory), log-interval, extensive ratio, cyclical ratio, derived ratio, counts and absolute (e.g. based on Dempster–Shafer theory).

Based on these works and for the purposes of quantitative assessment of operational risk we propose the adoption of selected scales, which are shown in Table 2.9. The choice of the scale type depends on many factors, among which the most important include: the specifics of the system under consideration, the type of threat and the knowledge maturity. Decision-makers can estimate the risk attributes using a range of historical, analytical, or subjective measures. They categorize potential risks by their consequences and likelihoods, creating risk matrix. Figure 2.14 shows an example of the generalized 2×2 risk matrix, in which four domains have been distinguished. Each of them has a different decision situation and therefore, also different risk assessment methods. In square A, for low

Table 2.9 Four levels of measurement and their characteristics

Scale/provides	Nominal	Ordinal	Interval	Ratio
Order of values		x	x	x
Mode	x	x	x	x
Median		x	x	x
Mean			x	x
Additivity			x	x
Multiplicativity				x
Has true zero				x

likelihood and low consequences of the risky scenario, we are dealing with minor incidents, that can be dealt with qualitative, reactive and operational-oriented approach. Square B corresponds to the situations with high likelihood and low consequences of the risky scenario, therefore typical for common failures and faults. In these cases, the right way to proceed is the quantitative, statistical, availability-oriented approach, as will be shown in the Sect. 4.1 (Infrastructure reliability creating—concept of High Reliability Organization). In square C, for high likelihood and high consequences of the risky scenario, we are dealing with serious failures and accidents. The right way to proceed in these situations is the combined, reactive, dependability-oriented approach, as will be shown in the Sect. 4.3 (concept of Dependable Operating). The last of the squares—area D—responds to a low likelihood and high consequences of the risky scenario. This is an area of rare disasters and catastrophes, that should be managed with qualitative, adaptive, resilience-oriented methods. This will be the subject of the Sect. 4.1 (Process continuity assurance—concept of Resilient Enterprise).

The third attribute—knowledge measure—decides which combination of consequence measure and uncertainty measure can be considered as acceptable and which cannot. We propose the use of the knowledge maturity concept (described in the Sect. 2.1.4) in order to final risk assessment according with the model (2.43). A simple example of this method application is shown in Fig. 2.14, in which the CL symbol is marked by the level of consequences C, and PL by the uncertainty level P. If the level of knowledge is low (L), only situations corresponding to the combination of CL = (1, 2) and PL = (1,2) are allowed, which corresponds to fields with blank background in Fig. 2.14. In the case where the level of knowledge is moderate, the situations corresponding to the combination of C = (1, 2, 3) and P = (1, 2, 3) are acceptable, which corresponds to fields with blank background and with the dotted background in Fig. 2.14. However, if the level of knowledge is high, the situations corresponding to the combination of C = (1, 2, 3, 4) and

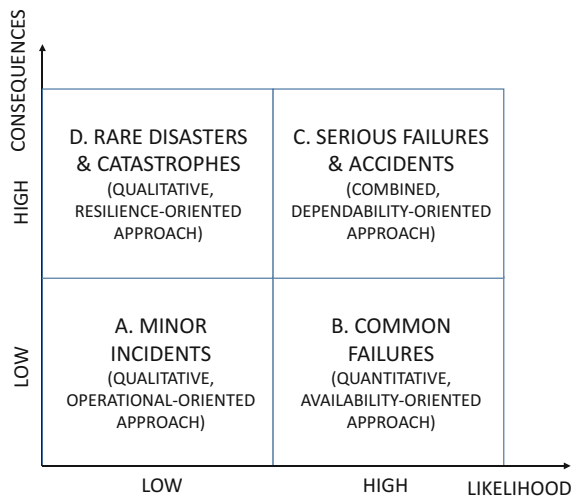


Fig. 2.14 Categorizing potential risks with a generalized 2 × 2 risk matrix

PL /CL	CL = 1	CL = 2	CL = 3	CL = 4	CL = 5
PL = 1					
PL = 2					
PL = 3					
PL = 4					
PL = 5					

Fig. 2.15 An example of the extended risk matrix

P = (1, 2, 3, 4) are acceptable, which corresponds to fields with blank background, with the dotted background and with the oblique lines background in Fig. 2.15. The chequered area corresponds to the combinations that cannot be accepted under any circumstances.

References

- Ackoff RL (1989) From data to wisdom. *J Appl Syst Anal* 16:3–9
- Adams J (1995) *Risk*. UCL Press, London
- AIAG (2008) Potential failure mode and effects analysis (FMEA). Appendix E
- Al Shalabi L, Shaaban Z, Kasasbeh B (2006) Data mining: a preprocessing engine. *J Comput Sci* 2 (9):735–739
- Aven T (2012) The risk concept—historical and recent development trends. *Reliab Eng Syst Saf* 99:33–44
- Aven T (2015) *Risk analysis*. Wiley
- Bargiela A, Pedrycz W (2002) *Granular computing*. Kluwer Academic Publishers
- Basel Committee on Banking Supervision (2008) Range of practices and issues in economic capital modelling. <https://www.bis.org/publ/bcbs143.pdf>
- Beer M, Möller B (2013) *Fuzzy randomness: uncertainty in Civil Engineering and Computational Mechanics*, Springer
- Bergmann G (1957) *Philosophy of science*. University of Wisconsin Press, Madison, WI, US
- Bukowski L (2015) Concept of the generalized model of quantitative risk assessment. *Forum Sci Oecon* 3(2):5–16
- Chrisman NR (1998) Rethinking levels of measurement for cartography. *Cartogr Geogr Inf Sci* 25 (4):231–242
- Corrigan D (2013) Integrating and governing big data. IBM Corporation Software Group
- de Moivre A (1738) *Doctrine of chances*. Chelsea Publishing, New York
- Dubois D, Prade H (eds) (1996) *Fuzzy information engineering: a guided tour of applications*. Wiley
- Eusgeld I, Freiling FC, Reussner R (eds) (2008) *Dependability metrics*. Springer, Berlin, Heidelberg
- Filev D, Yager RR (1994) *Essentials of fuzzy modeling and control*. Wiley-Interscience
- Hardy CO (1923) *Risk and risk bearing*. University of Chicago, Chicago, p 1
- Hartley RVL (1928) Transmission of information. *Bell Syst Tech J* 7(3):535–563
- Irwin T (1988) *Aristotle's first principles*. Clarendon Press, Oxford
- ISO (2009) *Risk management—principles and guidelines*. ISO 31000:2009
- Jamshidi M, Tili A, Zadeh LA, Boverie S (eds) (1997) Applications of fuzzy logic—towards high machine intelligence quotient systems. In: *Environmental and intelligent manufacturing systems series*, vol 9. Prentice Hall, Upper Saddle River, NJ
- Kaplan S, Garrick BJ (1981) On the quantitative definition of risk. *Risk Anal* 1:11–27
- Kirch W (ed) (2008) Level of measurement. In: *Encyclopedia of public health*. Springer, pp 851–852
- Klimko G (2001) Knowledge management and maturity models: building common understanding. In: *Proceedings of the second European conference on knowledge management*, Bled, Slovenia, pp 269–278
- Klir GJ (1987) Where do we stand on measures of uncertainty, ambiguity, fuzziness, and the like. *Int J Fuzzy Sets Syst* 24:141–160
- Klir GJ (2004) Generalized information theory: aims, results and open problems. *Reliab Eng Syst Saf* 8:341–354
- Klir GJ, Yuan B (1995) *Fuzzy sets and fuzzy logic: theory and applications*. Prentice Hall, PTR, Upper Saddle River, NJ
- Knight FH (1921) *Risk, uncertainty, and profit*. Houghton Mifflin Co., Boston
- Kulikowski JL (2014) Data quality assessment: problems and methods. *Int J Organ Collect Intell (IJOICI)* 4(1):24–36
- Mendel JM (2001) *Uncertain rule-based fuzzy logic systems*. Upper Saddle River, NJ: Prentice Hall PTR
- MITRE (2014) *Systems engineering guide*. The MITRE Corporation. <https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf>

- Nguyen HT, Kreinovich V, Di Nola A (2003) Which truth values in fuzzy logics are definable. *Int J Intell Syst* 18(10):1057–1064
- Pedrycz W, Gomide F (1998) Introduction to fuzzy sets. MIT Press, Cambridge, MA
- RIMS Executive Report (2011) Exploring risk appetite and risk tolerance. https://www.rims.org/resources/ERM/Documents/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf
- Ross TJ (2004) Fuzzy logic with engineering applications. Wiley
- Rumsfeld D (2011) Known and unknown: a memoir. Penguin Group, New York
- Shannon CE (1948) The mathematical theory of communication. *Bell Syst Tech J* 27
- Shaw BE, Carlson JM, Langer JS (1992) Patterns of seismic activity preceding large earthquakes. *J Geophys Res Solid Earth* (1978–2012) 97(B1):479–488
- Skyttner L (2008) General systems theory. Problems, perspectives, practice. Word Scientific
- Sornette D (2009) Dragon-kings, black swans and the prediction of crises. *Int J Terraspace Sci Eng*. <http://www.arxiv.org/physics>
- SRA Glossary (2015) <http://www.sra.org/sites/default/files/pdf/SRA-glossary-approved22june2015-x.pdf>
- Taleb NN (2010) The Black Swan: the impact of the highly improbable. Penguin Books, London
- Utkin LV (2004) A new efficient algorithm for computing the imprecise reliability of monotone systems. *Reliab Eng Syst Saf* 86(2004):179–190
- Walley P (1991) Statistical reasoning with imprecise probabilities. Chapman and Hall, London
- Weerdmeester R, Pocaterra C, Hefke M (2003) Vision: next generation knowledge management: knowledge management maturity model. Information Societies Technology Programme
- Yen J, Langari R (1998) Fuzzy logic: intelligence, control and information. Prentice Hall, Berlin
- Zadeh LA (1965) Fuzzy sets. *Inform Control* 8:338–353
- Zadeh LA (1973) Outline of a new approach to the analysis of complex systems and decision processes. *IEEE Trans Syst Man Cyber SMC* 3:28–44
- Zadeh LA (1978) Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets Syst* 1:3–28
- Zadeh LA (2005) Toward a generalized theory of uncertainty (GTU)—an outline. *Inf Sci* 172:1–40

Chapter 3

Describing Engineered Systems



Simplicity is the ultimate sophistication.

Leonardo da Vinci.

3.1 Infrastructures—Topology-Based Methodology

3.1.1 System Approach—Systems Engineering

The second half of the twentieth century has witnessed the rise of a new scientific meta-discipline called *systems science*, mainly based on holism, synthesis, as well as reductive and inductive reasoning. Systems sciences have a specific view of the world, relying on the quest to understand man and his environment as mutually interacting elements of one system, elements examined from multiple perspectives and in different ways, but always as a single whole. Various systems theories, as well as the general systems theory (von Bertalanffy 1955) have emerged on the basis of systems sciences. The general systems theory currently serves as a universal language which brings together various areas of interdisciplinary communication. General systems theory, also known as the theory of general systems, is still under constant development, striving to create the foundations of a universal science based on the so-called “law of laws” which will integrate all areas of scientific knowledge. In 1956, Boulding (1956) has very aptly formulated its role as follows:

General Systems Theory is the skeleton of science in the sense that it aims to provide a framework or structure of systems on which to hang the flesh and blood of particular disciplines and particular subject matters in an orderly and coherent corpus of knowledge.

Systems sciences have developed a new scientific paradigm called holism, that is, *systemic approach*. Systemic approach looks at the whole through the role and function of parts in the whole, taking into account the relationship of cause and effect (often undisclosed, non-linear and distant in time). It is characterised by a turn:

- from an emphasis on the part to focusing attention on the whole,
- from a static structure to a dynamic and process structure,
- from a metaphor of a hierarchical structure or a linear chain to the metaphor of a network,
- from the desire for an absolute truth to the approximate description.

The foundation for the systemic approach is *systems thinking* (Gharajedaghi 2006; Klir 1969; Weinberg 1975), based mainly on synthetic research procedure which, somewhat simplified, can be reduced to three following steps:

- identification of the entire system, which includes the examined elements (e.g. subsystems),
- evaluation and description of the system's properties and its behaviour in time,
- determination of the properties of an individual system's elements and their behaviour in time, taking into account the impact of these elements on the implementation of system's functions.

The main task of this kind of synthesis is not a precise identification of the system's structure, but rather gaining knowledge about its behaviour in time and—in particular—about its functions. Thus, the cognitive emphasis of systemic synthesis is placed at explaining (what?) and understanding (why?) the behaviours and functions of the system, with a particular emphasis on variability in time, while an analytical approach focuses on determining static (fixed in time) structural characteristics of the system.

Systemic approach gained significance in recent decades, due to the growing number of the so-called large-scale problems. These include important issues in both defence and civilian systems, in terms of production and services, and examined from different perspectives—technical, economic, social, environmental and political. The root of these problems lies in complex interactions between the elements and states of the system, as well as unpredictable changes in the environment caused by forces of nature (natural disasters) or deliberate criminal and terrorist activity. Large-scale problems lead to the phenomenon of *the mess*, defined by Russell L. Ackoff, who in his book (Ackoff et al. 2006) defines the mess as a state of an organisation (a system) caused by a combination of unexpected and interrelated situations that pose a threat (danger) or a chance (opportunity) to the organisation. A lack of response to the mess, or limiting oneself to partial (non-systemic) solutions can lead to a deep crisis or even a total destruction and collapse of the entire system. Classic methods of solving such problems are generally ineffective, which is a result of the so-called circular logic effect, among others. This effect consists in the fact that in complex systems with a large number of interactions between elements and state variables, certain system states can be both the causes and effects of changes taking place in the system. This is what makes it difficult to identify both the problem itself and the causes that could lead to it.

The practical implementation of the idea of a systemic approach is now possible thanks to the dynamic development of information technology. It requires a synergetic cooperation in numerous areas using a variety of methods and tools, e.g. in

accordance with the so-called **C⁴I²** principle, whose name is an acronym for the following terms: **C**ommand, **C**ontrol, **C**ommunication, **C**omputer, **I**ntegration, **I**ntelligence. The main objective of this rule is to support decision-makers in handling unexpected situations, which they have never had to deal with (Skyttner 2008).

During the work on the development of general systems theory, a number of proposals have been made for defining the concept of the system. In *An Approach to General Systems Theory* (Klir 1969), George J. Klir made a critical analysis of the applied ways of defining systems and proposed a new approach to the problem, which he referred to as *inductive approach* (as opposed to deductive approach dominating in that time). This approach was based on distinguishing four basic features of systems, namely: the resolution level of examined system values (i.e. the accuracy and frequency of measurement), behaviour over time (variability of system values observed over time), relations stable over time (the relationships between system values that are stable over time) and properties describing these relations. As a result, a classification of definitions was created. It includes the following five types (classes):

1. A given system is a set of values examined at a certain resolution level.
2. A system is a set of values representing the variability of values under consideration over time.
3. A system is a given relation, stable over time, between instantaneous and/or past and/or present external values.
4. A system is a given set of elements and their regular behaviour and the set of forces between individual elements and between the elements and the environment.
5. A system is a set of states and a set of transitions between states, where these transitions may be indeterministic in nature.

In the application of systems theory to practical problems (e.g. in systems engineering) the last two definitions proved to be the most useful—the first one (no. 4) is called a UC definition (Universe of Discourse and Couplings), whereas definition no. 5 is a ST definition (State Transition). Both are structural in nature and can be described in one general mathematical model in the following form (Klir 1991):

$$S \subset (E \times R) \quad (3.1)$$

where:

- S modelled system
- E elements of the system,
- $\times$ Cartesian product,
- R relations between system elements.

This model can be regarded as universal, if we assume a generalised interpretation of the symbols E and R . Then the E elements of the system can be its parts

(material or intangible objects), events, states or functions, whereas R relations may apply both to relations between different elements (e.g. in hierarchical systems) and forces such as mutual interactions and interactions in dynamic systems (e.g. in a process approach—flows of matter, energy and information).

The theories with the highest level of generality include mathematical systems theories, in which the basic characteristics of the systems are derived directly from formal definitions of the notion of a system. *Mesarovic's theory* (Mesarovic 1972) is an example of such a theory. Mesarovic examines the properties and behaviour of the systems using formal methods and introduces basic concepts to the theory in the form of axioms. The theory is based on the principles of formal logic and is cybernetic in its nature. It is based on the concepts of *information processing* and *decision-making*. It allows for an adequate description of multi-level, hierarchical decision-making systems and lays the foundations for the analysis and synthesis of control systems.

Formalising the description of the system takes place in two stages:

- Verbal (linguistic) formulation of the system's definition, consistent with the intuitive meaning of the system in the examined fields of study and fields of application
- Axiomatic defining of previously formulated concepts, using lowest possible mathematical structure

Mesarovic has formulated the definition of a generalised system in the following manner:

General system S is a relation defined on abstract sets

$$S \subset \times(V : i \in I) \quad (3.2)$$

where $\times$ is the Cartesian product, I is a set of i indexes, and V is a set of V_i relations.

When I is a finite set, the formula is simplified to:

$$S \subset (V_1 \times V_2 \times V_3 \times \dots \times V_n) \quad (3.3)$$

where the components of the V_i relations are called the system's objects.

Each object represents a feature or a characteristic of the system, expressed in terms which describe the given system, and the V sets includes all possible ways a given feature can be perceived or observed. A system, therefore, is the entirety of possible combinations in which the system's objects can appear.

Mesarovic distinguishes two linguistic categories:

- Nouns denoting objects and
- Functors denoting relations between objects.

These categories allow for a description of the system in case the information about it is incomplete. If full information about the behaviour of the system is available, a *behavioural description*, or *cause and effect description*, of the system can be used, namely:

Input (stimulus)

$$X = \times(V_i : I_x) \quad (3.4)$$

Output (reaction)

$$Y = \times(V_i : I_y) \quad (3.5)$$

The system is then a relation determined on a set of inputs and outputs

$$S \subset (X \times Y) \quad (3.6)$$

Therefore, for a full description of a system in this approach, one requires to know all possible inputs (causes or stimuli) and corresponding outputs (effects, reactions or responses of the system).

Another way of describing a system is the so-called *teleological (finalistic) description*, that is, *description through striving towards a goal*, which became the starting point for the so-called process approach. It distinguishes X inputs and Y outputs, whereas the behaviour of the system is not described by specifying the procedure determining the relationships between stimuli and responses, but in terms of the process of pursuing goals (i.e. as if the system reacted to a given stimuli in such a way as to achieve the intended purpose). Formalising this method of description requires, aside from X and Y , the introduction of additional objects: decision objects— M and value objects V and two functions:

- *The performance function* of pursuing goal process

$$P : X \times M \rightarrow Y \quad (3.7)$$

- *The goal function* characterising the process of pursuing goal

$$G : M \times Y \rightarrow V \quad (3.8)$$

Therefore, the pursuit of a goal in this case is the control or management of a system with an intent to achieve the desired (expected) result P , while optimize the G function. If the G function is a measure of the resources used to achieve the goal (e.g. a function of costs), then control should aim to minimize it, whereas if G function is a measure of the process' *efficiency*, then control should ensure the maximization of the G function. The performance function P can be a *effectiveness* measure of the pursuing goal process, understood as the degree of implementation of the desired objective.

As the concepts of effectiveness and efficiency are widely used in management sciences, therefore it is assumed further in the paper that in terms of Mesarovic's theory, the performance function P will be a measure of effectiveness of a process implemented by a given system, and the goal function G will be identified with the efficiency of the process.

Russell L. Ackoff proposed to organize the systems concepts by publishing an article titled “Towards a System of Systems Concepts” in 1971 in the *Management Science Journal* (Ackoff 1971). The publication is a framework, which comprises 32 points defining the basic concepts in the theory of systems, the relations between them and a classification of systems in a behavioural approach. The concept of system has been defined as follows:

System is a set of interrelated elements. Thus a system is an entity which is composed of at least two elements and a relation that holds between each of its elements and at least one other element in the set. Each of a system's elements is connected to every other element, directly or indirectly. Furthermore, no subset of elements is unrelated to any other subset.

The basic division of systems, based on their relation to reality, distinguishes two types of systems: abstract and concrete. *Abstract systems* are characterised by the fact that all items included in their composition are intangible. Relations between abstract elements are defined using assumptions in the form of postulates or axioms. Examples of such systems include natural and programming languages, philosophical and classification systems. *Concrete systems* are those in which at least two elements are material objects. They are a study subject for systems engineering, which is a field of application of knowledge based on systems theory and the subject of interest of this paper.

Every concrete system, at any moment in time, can be described by a set of its properties (characteristics). *The state of a system* at t_i moment is the set of relevant properties which the system has at that time. A set of system states may be infinite, but in extreme cases it can be reduced to two states important for the observer (e.g. suitable—unsuitable, moving—resting, meeting the requirements—not meeting the requirements).

The environment of a system is a set of elements and their relevant properties, which are not part of the system (they are outside its borders) but may influence (substantially) the state of the system. *The state of a system's environment* at t_i moment is a set of the relevant properties of its environment at that time.

Depending on the severity of the environment's impact on a given system, systems are divided into closed and open systems. A *closed system* is one that has no environment, that is, no element outside of the system has a significant impact on the state of the system. The state of an *open system* depends on both the properties of the system and its environment.

The properties of the system and its environment, and more specifically, their values may change over time. Such important changes to at least one structural property of the system and its environment are called *events*. A *static system* (one-state system) is one where no events occur, therefore it is unchanging over time. *Dynamic systems* (multi-state systems), are ones where events occur and whose state changes overtime. The events which have a decisive influence on the changes taking place in systems are: reaction, response and act. A *reaction* of a system is an event for which another event, preceding it, that occurs to the same system or its environment is necessary and sufficient. A *response* of a system is an event for which another event, preceding it, that occurs to the same system or to its

environment is necessary but not sufficient. For a system “response” to take place it is therefore necessary that an additional stimulating event, a co-producer, has to occur in another system or its environment. *An act* of a system is an event that occurs without external stimuli as a self-determined action caused by the system itself.

The division of systems according to the basic criteria such as the origin of the system, its relation to reality, its content, relation to the environment, degree of determinacy, complexity, variability in time, continuity and role are presented in a dichotomous approach in Table 3.1.

A system’s behaviour is a sequential chain of changes to the system occurring as a result of preceding events such as: reactions, responses and acts. These changes can therefore initiate other events in the system or its environment. In order to describe the behaviour of a system it is necessary to know both the significant events preceding a given moment, as well as the consequences of these events. Depending on how the system reacts to these events, or behaves, four basic kinds of systems can be distinguished: *passive* (with a *static behaviour*) as well as *reactive*, *responsive* and *active* (with *dynamic behaviour*) systems. Table 3.2 contains a short description of behaviour and relation to goal of these individual types of systems, with simple examples. From the standpoint of practical application in production and services, including logistics, the *goal-seeking* and *purposeful systems* are particularly interesting. Smart and creative control and management of such

Table 3.1 The dichotomous division of systems according to the basic criteria (based on Bukowski 2016)

Criterion	Dichotomous division	
Origin	Natural	Artificial
Relation to reality	Concrete	Abstract
Substance	Material	Immaterial
Relationship with the environment	Closed	Open
Degree of determinacy	Deterministic	Indeterministic
Degree of complexity	Single	Multiple
Variability in time	Static	Dynamic
Continuity	Discrete	Continuous
Fulfilled function	Operating	Configuration

Table 3.2 The basic types of systems and their main characteristics (based on Bukowski 2016)

Type	Behaviour	Relation to goal	Example
I—Passive	Static	Fixed	Tool
II—Reactive	State-maintaining	Variable (given)	Thermostat
III—Responsive	Goal-seeking	Variable (chosen)	Autopilot
IV—Active	Purposeful	Adaptive	Critical infrastructure networks

systems require the use of structures with autonomous elements, connected by relations allowing for mutual communication (exchange of information) in real time.

The purposefulness (or in the case of operational systems—functioning) of these systems is based on pursuing a certain state which can be defined in a strategic and operational scale. The notion of *functioning* (or *operating*) is understood as a manifestation of rational behaviour, involving the fulfilment of certain (required) functions, e.g. the execution of production processes or services. The purpose of an operational system should be to fulfil the expectations of the object of the action (owner, customer, society). *The goal* of an active system is the preferred state of a system, guaranteeing the production of a given functions at the outcome within a specified, relatively short time period. *The objective* of an active system is the preferred state of the system, guaranteeing the production of a given function in an ultimately desirable degree in a long period of time (a long-term goal).

The function of a system is to generate (produce, achieve) results in line with the goals and objectives of the system, regardless of the state of the system and its environment. In practice, the function of production systems is the effective and efficient production of certain products, whereas service systems come down to providing services in accordance with the requirements of the customers at prices (costs) favourable to both sides.

Figure 3.1 depicts a general model of a real engineered system with a defined structure and dynamic behaviour. Its inputs are the events occurring in its environment (controllable—resources supply, as well as uncontrollable—disruptions), and its outputs are the produced functions (controllable—goods and services delivery, as well as uncontrollable—disruptive events).

In practice, *organisations* comprise a very important class of systems. We adopt the following general definition of an organisation:

An organisation is a controllable, function-producing and goal-seeking entirety, which is separate from its environment and whose elements are connected by mutual relations, both physical and intangible.

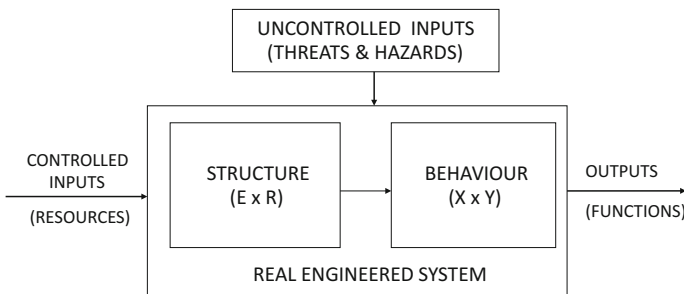


Fig. 3.1 General model of a real engineered system

The function of an organisation is to effectively and efficiently complete the pursued goals. Material relations are the flows of goods (raw materials, semi-finished products, finished products and energy) between the elements of the organisation. Intangible relationships are communication, ensuring the flow and exchange of information between the elements of the organisation.

3.1.2 *Complexity and Emergence—System of Systems and Network Organisation*

In practice, one of the most important criteria of real systems division is the degree of their complexity (Table 3.1). In accordance with the definition of a system shown in Sect. 3.1, every system is composed of elements, which can be both simple objects with clearly defined properties, as well as whole systems consisting of individual objects. In the first case we are dealing with *single systems* (simple or complicated), and in the second with *multiple, complex systems*, often referred to as *systems of systems* (Gideon et al. 2005; Luzeaux et al. 2011). The main difference between these two classes of systems is that in the case of single systems, their properties are determined by the properties of their components and the nature of internal relations between these elements, whereas the properties of complex systems are emergent over the course of their operation (Eusgeld et al. 2011).

The mathematical model of such complex systems can be described as following:

$$\mathcal{S} = \{S_1, \dots, S_i, \dots, S_k\} \quad (3.9)$$

$$\mathcal{S} \subset (S \times \mathcal{R}) \quad (3.10)$$

where:

- $\mathcal{S}$ modelled complex system (e.g. system of systems),
- S set of subsystems,
- S_i subsystem i (element of the complex system),
- k number of subsystems,
- $\times$ Cartesian product,
- $\mathcal{R}$ relations between subsystems S .

The concept of emergence comes from the Latin word ‘emerge’, which means ‘to arise’. It describes the phenomenon of formation of qualitatively new structures and behaviours in the framework of complex systems resulting from interactions between a number of simpler objects forming the structure of these systems. The concept of emergence is crucial in the description of relevant properties of complex systems. It is based on the so-called ‘6 N’ rule and refers to features such as: novelty, non-reducibility, non-deducibility, non-predictability, non-computability, non-explainability. According to Mill (2002), emergence is the inability to

designate a certain value related to the total result of causes operating together, as a resultant of relevant values related to individual causes, based on a specific rule for composing given values. A system has emergent properties if the following conditions are met:

- it is impossible to explain the appearance of the emergent property on the basis of knowledge about the components of a complex structure, which they form (epistemic emergence),
- we are also not able to explain the emergent property on the basis of knowledge about the relationship between the components (interactive emergence),
- it is impossible to predict the existence of the emergent property when having knowledge of the characteristics of these components (actualizing emergence).

In real systems, emergence refers to phenomena observed in macroscopic scale, rather than occurring in microscopic scale. The examples of emergent systems include gatherings of living organisms such as ant colonies, termite mound, swarms of bees, bird V formation, schools of fish, flocks of wolves and even crowds of people.

The complexity of systems is multidimensional in nature, namely:

- structural,
- spatial,
- temporal and
- disciplinary.

Structural complexity is a function of the total number of elements that make up the system, the number of different types of elements that form the structure of the system and the number of active connections between the elements of the system. Unfortunately, there are no simple quantitative dependencies between these parameters, which would allow to determine the boundaries between single and complex systems. The only criterion is the fact that at least one of the above conditions has been met.

Spatial complexity is related with the system's spatial scope, that is, with the scope the system covers. In the case of economic and technical systems one usually distinguishes small scale systems, covering the scope of a single company, large scale systems (e.g. regional supply networks), very large scale systems (e.g. national critical infrastructure) and ultra large scale systems (e.g. global supply networks).

Time complexity is a result of the variability in the system's behaviour over time. Static and quasi-static systems represent a low level of complexity. A higher level of time complexity is assigned to dynamic systems of regular variation (e.g. periodic), and the highest level to dynamic systems with irregular variation (e.g. random or chaotic).

From the perspective of a discipline of science, which possesses knowledge of a given system, one can graduate complexity according to the following hierarchy:

- systems within a single discipline—monodisciplinary systems,
- systems within many scientific disciplines—multidisciplinary systems,
- systems on the border of defined scientific disciplines—interdisciplinary systems, and
- systems that exceed all boundaries between disciplines and combine all of the above features in an inclusive way—transdisciplinary (or over-disciplinary) systems.

In practice, complex systems such as systems of systems (SoS), are characterised by nonlinear structures (e.g. networks), spatial scope of at least a large scale, dynamic behaviour, especially responsive, and active, in particular (in accordance with the classification from Table 3.2) and going beyond a single scientific discipline (most commonly these systems require an interdisciplinary and transdisciplinary approach). Due to the fact that research methods used in classical systems engineering are insufficient for the analysis, synthesis and control and management of these types of systems, the so-called *system of systems engineering* has been developing for several years in parallel to single systems engineering. Table 3.3 shows, in a simplified manner, how important are the differences between these two areas of knowledge. It contains the dominant properties (attributes) of systems in terms of both research approaches.

The presented comparison shows that in addition to already enunciated differences between these approaches, one should pay attention to the multiplicity of goals that occur in complex systems, limited capabilities of finding solutions within these systems (searching for satisfactory solutions instead of optimization) and extending the time horizon in the research of complex systems from the scope of a lifespan to a virtually limitless one (as a result of the pursuit of sustainability).

Table 3.3 Comparing the main attributes of system engineering and system of systems engineering (based on Jashidi 2009; Souza-Poza et al. 2008; Valerdi et al. 2008; Zio 2007)

Attribute	System engineering	System of systems engineering
Focus	Single complex system	Multiple integrated complex systems
Problem	Defined	Emergent
Objective	Optimization (best)	Satisfying (good enough)
Boundaries	Static (fixed)	Dynamic (variable)
Structure	Hierarchy	Network
Goal	Unitary	Pluralistic
Approach	System related	Methodology related
Timeframe	Life cycle	Continuous
Design tools	Many	Few
Standards	Few	Non

The main characteristics of a SoS are:

- multidimensional complexity—nonlinear and heterogeneous structures (e.g. networks), spatial scope of at least a large scale, dynamic behavior, and going beyond a single scientific discipline (interdisciplinary or transdisciplinary approach),
- operational and managerial independence of its elements (subsystems)—the subsystems must be able to usefully operate independently and maintain a continuing operational existence independent of the SoS,
- emergent behavior—the SoS performs functions and carries out purposes that do not reside in any subsystem,
- evolutionary development—development and existence of SoS is evolutionary with functions and purposes added, removed, and modified with experience.

The typical SoS is composed of three main kinds of systems: infrastructure implementing the required functions (e.g. the network organization), protection subsystem (safety and security) and meta-system of management (the flow of information and communication within the SoS). Examples of such SoS can include e.g. power supply networks (smart grids), the Internet of things, telecommunication networks and global supply chains. They are characterized by the following qualities: a distributed structure, a high degree of autonomy of the individual components (agents), a multi-state dynamics, emergent properties and the ability to keep up with rapidly changing target (e.g. demand-driven supply chain).

On the basis of the above considerations, one can introduce the concept of a network organisation, which is the dominant structure in modern logistic systems. *Network organisation* is a structurally, spatially and temporally complex process organisation, whose elements comprise of independent enterprises, and its properties are emergent in their nature.

The main features of network organisations include (Bukowski 2016):

- Flat (horizontal) structure with the topology of a weighted digraph, with blurred borders between the organisation and its environment.
- Spatial scope reflecting the scale of the organisation extending beyond one company.
- Variation in time resulting from environmental dynamics and the shortening of the life cycle of products and services.
- The ability to change expressed by flexibility and agility, thanks to functional redundancy (simultaneous execution of processes).
- Synergy resulting from the full compatibility of competences of units forming the network organisation, the adoption of common goals and the organisational capacity to learn.
- A significant intellectual potential through knowledge sharing between the units of the network and emerging knowledge.

Due to the manner of exercising management functions, the structures of network organisations can be divided into: centralised, decentralised and distributed (see Fig. 3.2).

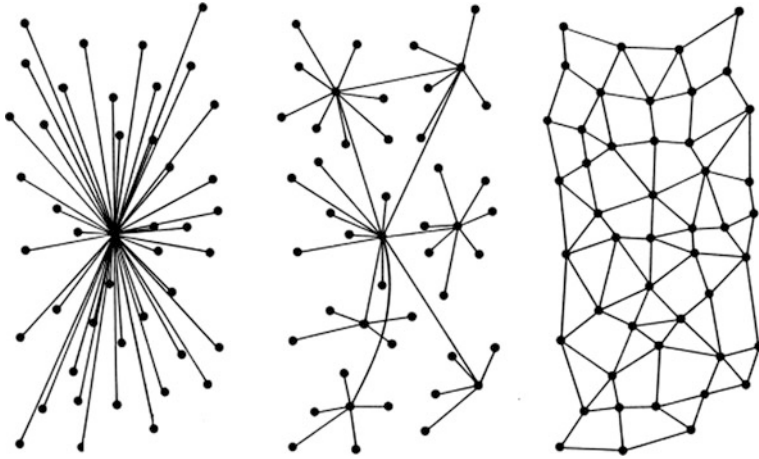


Fig. 3.2 Main types of network organization structures: centralized (on the left), decentralized (in the middle), and distributed (on the right)

In theory, the structure of complex networks can be described using graphs in the form of (Newman 2010):

$$G = (V, E) \quad (3.11)$$

where:

- G directed or undirected graph,
- V vertex (set of nodes in network),
- E edge (set of lines connecting two nodes).

In Fig. 3.2 black points indicate the nodes of the network, while the lines connecting these points are edges. According to the mathematical theory of graphs, the basic size describing the network node is the so-called *node degree* d . It defines how many ends of lines belong to a given node, i.e. how many of the given nodes have partners or neighbours. The frequency of occurrence of nodes with various degrees can be described by the binomial model (also called the Bernoulli distribution), which characterizes a network with N random connected nodes. These networks are called *random networks* of the ER-type (Erdos-Renyi model), and are created by adding each of the possible $N(N - 1)/2$ connections with a constant probability of P . However, ER-type networks are rare in the real world and in practice we usually find random networks described by the universal power-law (also called Pareto-law) with the following formula:

$$P(d) = a \cdot d^{-\alpha} \quad (3.12)$$

were:

- P probability of d ,
- d node degree,
- a constant value,
- α exponent's value (a number within the range 2–4)

Networks subjected to the power-law are called *scale-free networks* (Barabasi et al. 1999), and their important feature is that they are invariant to the operation of scaling the degree of nodes. This means that after changing the degree scale of nodes with a power distribution, their distribution is still described by the power-law. The topology of the scale-free network is usually characterized by the presence of a small number of nodes with high degrees d , so-called hubs, and a relatively large number of nodes with low degrees d . It causes that such a network is usually resistant to accidental failures and susceptible to precisely planned “attacks”. Figure 3.3 shows examples of the most common network structures: centralized, scale-free and random, with the same number of nodes.

There are also many modifications of these typical network structures, and one of the most popular is the so-called *small-world network* (Watts et al. 1998). This type of network is partially disordered, but not fully random. A small-world network is a type of system in which most nodes are not neighbours of one another, but the neighbours of any given node are likely to be neighbours of each other and most nodes can be reached from every other node by a small number of steps. The small-world network is defined as a network where the typical distance L between

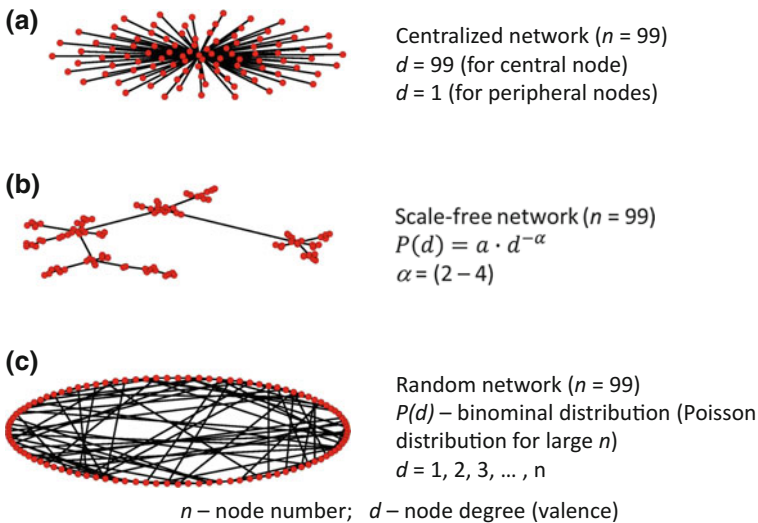


Fig. 3.3 The most common network structures: **a** centralized, **b** scale-free and **c** random, with the same number of nodes $n = 99$ (based on Dittes 2012)

two randomly chosen nodes (the number of steps required) grows proportionally to the logarithm of the number of nodes N in the network.

We can characterize all types of networks by defining basic measures for their properties. One of the most important uses of network analysis is identification of most central units in a network. *Measures of centrality* can be defined in two different ways (Newman 2010):

- for each unit respectively, as a unit centrality (one number for each unit), or
- for the whole network, as a network centralisation (only one number for the whole network).

When we describe the *network centrality* we have to distinguish between undirected and directed networks:

- the term centrality measures is used for undirected networks (a communication node is central, if a lot of roads are passing through it),
- the term prestige is used for directed networks. In this case we can define two different types of prestige: one for outgoing edges (measures of influence), and one for incoming edges (measures of support).

Unit Centrality—selected unit is central if: it has a high degree, it is easily accessible (close to) all other units, it lies on the shortest paths between other units.

Degree Centrality—a unit is central in a network, if it is active enough in the sense that it has a lot of links to other units. In the case of cycle all units are equally central. Degree centrality is defined by a degree of unit x :

$$c_D(x) = \text{degree of unit } x \quad (3.13)$$

Such measures are called *absolute measures of centrality*. Absolute measures cannot be used to compare centralities of networks with different number of units. Therefore such measures are normalised to get measure in interval from 0 to 1, where 0 means the smallest possible and value 1 the highest possible centrality. Measures normalised in this way are called relative measures of centrality.

Closeness Centrality—the measure of centrality according to closeness of unit x :

$$c_C(x) = 1 / \sum_{y \in U} d(x, y) \quad (3.14)$$

where $d(x, y)$ is the graph-theoretic distance (length of the shortest path) between units x and y , and U is set of all units. If network is not strongly connected, we take only reachable nodes into account, but we weigh the result with a number of reachable nodes. The most central units according to closeness centrality can rapidly interact with all others because they are close to all others. This measure is preferable to degree centrality, because it takes into account both direct and indirect connections among units.

Relative Closeness Centrality is defined by the formula:

$$C_c(x) = (n - 1) \cdot c_C(x) \quad (3.15)$$

The smallest possible distance of selected unit from all other units is obtained, if the unit has all other units for neighbours. In this case the absolute closeness centrality is $1/(n - 1)$. Closeness centrality can be calculated for undirected and directed networks. There are two possibilities for directed networks: prestige can be calculated according to outgoing edges (how close are all other units from the selected one; it corresponds to how many steps we can reach all other units from the selected one), or according to incoming edges (how close is the selected unit to all others; it corresponds to how many steps we need to reach the selected one from all other units).

Betweenness Centrality—in the case of communication networks the distance from other units is not the only important property of a unit. More important is which units lie on the shortest paths among pairs of other units. Such units have control over the flow of information in the network. The concept of betweenness centrality measures is based on the assumption that a unit is central, if it lies on several of shortest paths among other pairs of units. We can define the centrality measure of unit x according to betweenness in the following way:

$$c_B(x) = \sum_{y < z} \frac{\text{shortest path from } y \text{ to } z \text{ through } x}{\text{shortest path from } y \text{ to } z} \quad (3.16)$$

If communication in a network always passes through the shortest of available paths, then Betweenness Centrality of a unit x is the sum of probabilities across all possible pairs of units, that the shortest path between y and z will pass through the unit x .

3.2 Processes—Flow-Based Methodology

3.2.1 Process Approach—Service Engineering

A *service* can be described as: all intangible effects resulting from a client interaction that creates and captures value (ERISS 2016). Currently, services combine both products and services, and the distinction between the two is fuzzy and vague. Services are offered by a provider to its consumers. Baida defined business services as activities delivered by a service provider to a service consumer to create a value for the consumer (Baida et al. 2004). Business services are typically discovered and invoked manually, but their realization may be performed by automated or manual means. Services lack of concrete characteristics. Thus, services must be defined indirectly in terms of the effects they have on consumers. This makes the description of services one of the most important undertakings for the future.

Service knowledge is an area of expertise which involves: business, management, industrial engineering, information and communication technology (ICT), socio-legal sciences, and economics. *Service science* has developed in response to the need to combine technological and non-technological innovations in a rapidly growing and changing environment. The discipline focuses on the innovative creation of value by using various transdisciplinary approaches. A service-dominant approach is starting to take over from the traditional goods-dominant approach. Main key factors of the *service-dominant approach* include:

- the realization of a service as a process,
- a focus on dynamic resources,
- outsourcing and globalization,
- complex interdependences between elements.

Service science, management, and engineering (SSME) is a term introduced by IBM to describe service science, an interdisciplinary approach to the study, design, and implementation of service complex systems in which specific arrangements of people and technologies take actions that provide value for others. SSME has been defined as the application of science, management, and engineering disciplines to tasks that one organization beneficially performs for and with another (Sampson 2010). A *Service System* is a term that frequently appears in the service management, service operations, services marketing, service design, and service engineering literatures (Salvendy and Karwowski 2010). Service involves both a provider and a client working together to create value. These relationships and dependencies can be viewed as a complex system in which the parts interact with each other in a non-linear manner, and which have emergent properties. In many cases, the main source of complexity in a service system is its people: the client, the provider, or other organizations. The key to service science is multidisciplinary, focusing not merely on one aspect of service but rather on service as a system of interacting ideas from a number of existing disciplines—including computer science, cognitive science, economics, organizational behaviour, human resources management, marketing, operations research, and others—and aims to integrate them into a coherent whole.

Service engineering is a new methodology to the analysis, design and implementation of service-based ecosystems in which organizations and IT provide value for others in the form of services. Service Engineering not only provides methodologies to handle the increased complexity of numerous business actors and their value exchanges, but also provides tools for constructing and deploying services that merge the IT and business perspectives (Cardoso et al. 2009). Service Engineering is a structured approach for describing a part of an organization from a service perspective that expresses the way the organization works (Salvendy and Karwowski 2010). It provides a discipline for using models and techniques to guide the understanding, structure, design, implementation, deployment, documentation, operation, maintenance and modification of typical services as well as e-services. This approach should systematically translate an initial description from a natural

language that expresses the way stakeholders think and communicate about the organization through a sequence of representations using various models to a representation that is accepted and understood by all the participants of the system.

The explosive growth in services worldwide is seen as the next major challenge in the world economy. Because currently the powerful digital communications networks (such as the Internet) evolve rapidly, companies are transforming from regional businesses to globally integrated enterprises. With the ever increasing use of the Internet around the world, service networks using cloud computing will constitute the key ingredients for this generation. The fast-growing discipline of service engineering is related to service economy growth and the global need for innovation, developing and implementing of different kinds of services (Sampson 2010). Often the biggest problem lies in bridging the gap between business and IT. This challenge requires a set of design principles, patterns, and techniques that currently have not been identified precisely enough. Therefore, the *Internet of Services* cannot be realized without giving a strong emphasis on both the business as well as the technological side of services.

The *Unified Service Theory* (UST) developed by Scott E. Sampson could serve as theoretical background for building the general model of Service Engineering. The basis for a UST is the assumption that: “Services are production processes wherein each customer supplies one or more input components for that customer’s unit of production” (Sampson 2010). The Fig. 3.4a shows the theoretical model of a typical service based on this assumption, and the Fig. 3.4b the Unified Service Theory based model of the real service system (Bukowski et al. 2016).

The concept of a process is defined in standards (e.g. EN ISO 9000: 2015 and EN ISO 9001: 2015) and in professional literature in a variety of ways. On the basis

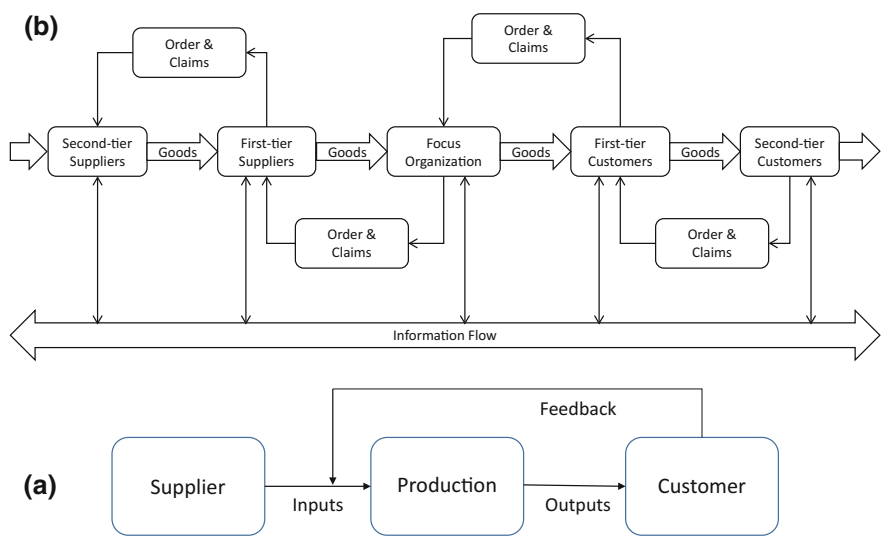


Fig. 3.4 Unified service theory based models of service systems (Bukowski et al. 2016)

of considerations made in previous sections, it is proposed to adopt two types of process definitions. The first one was based on the systems theory ST system definition. It is of formal nature and reads as follows: *A process is a system whose elements are events and activities connected by flow relations.*

Events are a change in the state of the system or its environment which can initiate the start of a process, interfere with it causing errors and pauses or end it when the desired outcome is achieved.

Activities are understood as intentionally designed and implemented actions. We divide them into:

- *Operations*, which apply to individual activities,
- *Tasks*, understood as sequences of activities or operations performed by the same “actor” on the same object, and
- *Decisions*, which are choices, as a result of which the process can branch into two or more paths.

Flows are relations that consist in the movement of goods (transport) and information (communication).

The process structure can be described in the form of a *PS* graph as following:

$$PS \subset (E, A, R) \quad (3.17)$$

where:

E process initiating, disturbing and terminating events,

A activities (operations, tasks, decisions),

R relations between events and flow relations.

The components of the structure can be set up in the following form:

$$E = (e_i : i = 1, 2, 3, \dots, l) \quad (3.18)$$

$$A = (a_j : j = 1, 2, 3, \dots, m) \quad (3.19)$$

$$R = (r_k : k = 1, 2, 3, \dots, n) \quad (3.20)$$

Business practice recommends using descriptive definitions, therefore the following definition of a process is proposed:

A process is a structured chain of events and actions interconnected by flow relations, the aim of which is to achieve the desired result.

The structure of a process defined in such a way can be understood as a configuration of events and activities connected by flows and represented by a sequential (chain type), parallelized (double- or multiple times), conditional (with XOR, OR, AND, COMPLEX logic gates) or mixed model. An exemplary structure diagram of such a process made in accordance with the BPMN (Business Process Modelling and Notation) notation is shown in Fig. 3.5. Individual symbols have the

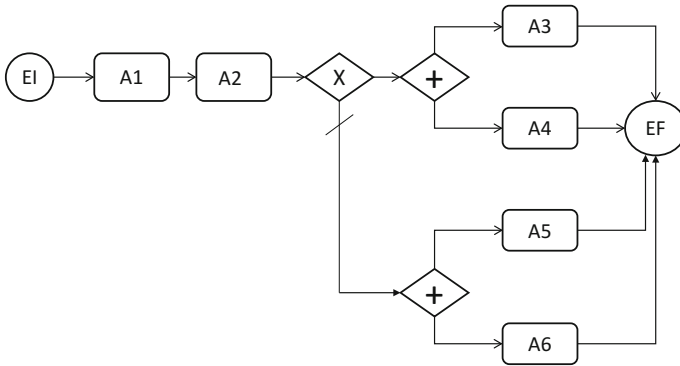


Fig. 3.5 An example of a process structure diagram made in accordance with the BPMN notation

following meanings: EI—initiating event, EF—final event, A1 to A6—activities, X—XOR gate, +—AND gate. The XOR gate means a choice which have only one correct solution (in this case, a yes/no choice). The OR gate differs from the XOR gate in that the process can be continued in more branches than only one. The AND gate indicates the possibility of branching the process and its further parallel implementation.

Process approach is to be understood as the identification of processes, their dependencies and order, determination of the criteria and methods ensuring and evaluating effectiveness, regular monitoring, measurement and analysis, as well as the implementation of any corrective actions necessary to achieve planned results and their continual improvement.

The classification of processes can be made on the basis of many different criteria, namely:

- Due to importance—basic processes and auxiliary processes
- Due to the level of decision-making—management processes and implementing processes
- Due to impact—strategic processes and operational processes
- Due to the creation of added value—processes creating added value and processes that do not create added value
- Due to the functional extent—inter-functional processes and cross-functional processes
- Due to hierarchy—main processes (macro processes) and second-rate processes (sub processes).

In practice, each process can be described by the following basic characteristics: name, supplier and client, goal (final result and partial goals), owner, structure (configuration model), input and output (cybernetic model), as well as the evaluation attributes and measures (parametric model).

In a cybernetic model one can distinguish two elements:

- Process input—material and intangible resources and other means necessary for the implementation of the process (resources, materials, information, financial resources),
- Process outputs—material and intangible resources, which are produced as a result of the process' completion (products, information, financial resources).

In a parametric model, the characteristics of a process are its attributes necessary to evaluate the ability of a process to deliver products and services with required features (characteristics). The most important include:

- Duration of the process—random variable T and its temporal structure (e.g. 10% taken by basic activities and 90% by auxiliary activities),
- Timeliness of the process—the compliance of the process' completion with the planned (fixed) deadline measured using absolute (ΔT) or relative ($\Delta T/T$) deviation.
- Quality of the process—expressed by a measure of client's satisfaction with the results of the process—multi-dimensional Q vector,
- Cost of the process—the structure and sum of all costs associated with the implementation of the process—process cost accounting using Activity Based Costing (ABC) method
- Flexibility of the process—the ability to undergo change and the used resources' susceptibility to transformation,
- Agility of the process—the speed of adaptation to changing external (e.g. in response to a customer's new request) or internal conditions.

Process organisation is a company formed and managed through the activities carried out by this company, i.e. processes. These processes should be closely aligned to both the dynamics of the changing environment, as well as to the internal structure of the company. It forces departure from functional structures of a static nature, to process structures characterised by a dynamic nature.

3.2.2 *Delivery Processes—Supply, Demand and Distribution*

Delivery process is a business cycle with many stages, such as getting a lead, turning the lead into a prospect, working towards the sale, closing the sale, and then delivering what was promised. This process is usually going on at various levels of organization. Delivery management (What 2018) is the organization, administration, and supervision of the people, processes, and technologies, which when combined into a comprehensive plan, provides the business and technical functions needed to successfully achieve what a client expects to receive. The person responsible for this type of work is referred to as the delivery director, delivery vice president, delivery manager or account manager depending on the organization.

There are many likenesses between a project manager and delivery director. Whereas the project manager will get into more of the details, the delivery director

oversees what is going on at a higher level and across more areas of responsibility. The delivery director anticipates the actions, thoughts, and directions of the client, and manages the client without them really knowing it.

Supply management is a strategic approach to planning for and acquiring the organization's current and future needs through effectively managing the supply base, utilizing a process orientation in conjunction with cross-functional teams (CFTs) to achieve the organizational mission (Monczka et al. 2009). The Institute for Supply Management defines supply management as the identification, acquisition, access, positioning, and management of resources and related capabilities an organization needs or potentially needs in the attainment of its strategic objectives. Supply management requires pursuing strategic responsibilities, which are those activities that have a major impact on long-term performance of the organization. These strategic responsibilities are not pursued in isolation, but should be aligned with the overall mission of the organization. The routine ordering and follow-up of basic operational supplies is not a strategic responsibility. The development of the systems that enable internal users to order routine supplies, however, is considerably more important. Supply management is a broader concept than purchasing. Supply management is a progressive approach to managing the supply base, and usually takes a process approach to obtaining required goods and services. We can describe supply management as the process of identifying, evaluating, selecting, managing, and developing suppliers to realize supply chain performance that is better than that of competitors (Monczka et al. 2009).

Delivery management is cross-functional process that involves purchasing, engineering, manufacturing, quality assurance, distribution, and other related functions working together as one team, to achieve further mutual goals. Instead of adversarial relationships, which characterize traditional marketing, delivery management features a long-term win-win relationship between a costumers and suppliers. Delivery management is a new way of operating, involving internal operations and external suppliers to achieve advances in cost management, product development, cycle times, and total quality control.

A *supply chain orientation* is a higher-level recognition of the strategic value of managing operational activities and flows within and across a delivery chain. A supply chain is a set of organizations linked directly by one or more of the upstream or downstream flows of products, services, finances, and information from a source to a customer. *Supply chain management*, then, involves proactively managing the two-way movement and coordination of goods, services, information. According to this, supply chain management requires the coordination of activities and flows that extend across boundaries. Supply chains are composed of interrelated activities that are internal and external to a firm. These activities are diverse in their scope; the participants who support them are often located across geographic boundaries and often come from diverse cultures. Although many activities are part of supply chain management, an improved perspective visualizes supply chains as composed of processes rather than discrete, often poorly aligned activities and tasks. A process consists of a set of interrelated tasks or activities designed to achieve a specific objective or outcome. New-product development, customer-order

fulfilment, supplier evaluation and selection, and demand and supply planning are examples of crucial organizational processes that are part of delivery chain management.

Regarding *supply chains as a series of systematic processes* makes sense for a number of reasons. Processes usually move across functional boundaries, which aligns well with a supply chain orientation. Well-communicated processes also accelerate learning, because organizations can document, measure, and improve their supply processes. Furthermore, supply chain processes can use best practices and knowledge that enhance the chance of success. According to Porter's value chain model we can conceptualize the supply chain as a subset of the value chain. The primary activities, or the horizontal flow across organizations, represent the operational part of the value chain, which can be referred to as the supply chain. At an organizational level, the value chain is broader than the supply chain, because it includes all activities in the form of primary and support activities. The original value chain concept focused primarily on internal participants, whereas a supply chain is both internally and externally focused; i.e. includes suppliers and customers who reside both upstream and downstream from the focal organization. To effective management of costs, quality, and delivery requires attention to suppliers that reside several tiers from the producer. The extended enterprise concept recognizes explicitly that competition is no more between firms but rather between coordinated supply chains or networks of firms.

Distribution management involves the processes of packaging, storing, and handling of materials at receiving docks, warehouses, and retail outlets. For complex products such as automobiles, which feature multiple goods, technologies, and processes, the supply chain becomes very complicated. The materials, planning, and logistics supply chain for an automotive company is shown in Fig. 3.6, which illustrates the complexity of the chain, spanning from automotive dealers back through multiple levels and suppliers tiers. The automotive company's supplier network includes the thousands 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 are sharing information only when there is trust between members. Thus, the management of relationships with other parties in the chain becomes very important. Organizations are effectively forming new types of relationships called partnerships or alliances that require sharing of resources. For instance, organizations may provide dedicated capacity, specific information, technological capabilities, or even direct financial support to other members of their supply chain so that the entire chain can benefit (Monczka et al. 2009).

Demand planning identifies all the orders on output. This includes forecasts of anticipated demand, inventory adjustments, orders taken but not filled, and spare-part and aftermarket requirements. Supply planning is the process developing a supply, production, and logistics network capable of satisfying demand requirements, based on the demand data. *Supplier relationships* are shifting from an adversarial approach to a more cooperative approach with selected suppliers. Supplier development, supplier design involvement, the use of full-service

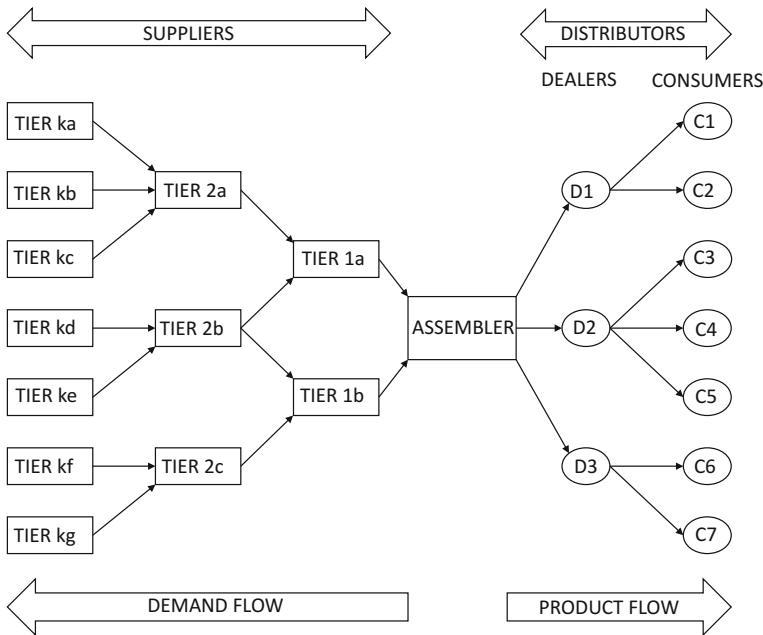


Fig. 3.6 The materials, planning, and logistics supply chain for an automotive company

suppliers, total cost supplier selection, long-term supplier relationships, strategic cost management, enterprise resource planning (ERP), integrated Internet linkages and shared databases can create new value within the supply chain. These trends will take time to occur fully with strong emphasis on *integrated supply chain management*.

Lean supply chains have their origin in the just-in-time concept, first adopted by many companies in the late 1980s. Just-in-Time (JIT) is a methodology of manufacturing based on planned elimination of all waste and on continuous improvement of productivity. It encompasses the successful execution of all operations activities required to manufacturing, from design engineering to delivery, and includes all stages of conversion from raw material to a final product. The main goals of Just-in-Time methodology are: to reduce the required inventory; to improve quality to zero defects; to reduce lead times by minimizing setup times, queue lengths, and lot sizes; to incrementally revise the operations themselves; and to accomplish these activities at minimum cost. In the broad sense, it applies to all forms of production, processes, and to many service industries as well. Firms following the JIT concept often experience remarkable improvements in their productivity, efficiency, and quality. This ability to do more with less led us to refer to JIT as *lean production*. It reflects the idea that the timing and level of inventory and production activities are closely matched to demand—*demand driven manufacturing*. The underlying principle of JIT—to eliminate all forms of uncertainty and waste—is relevant to each organization, regardless of the specific planning and control tools which it

uses. Using of some techniques such as Kanban is entirely possible if an organization follows the JIT methodology. A key rule of the JIT concept is a never-ending effort to eliminate waste ('muda', in Japanese), which is defined as "any activity that does not add value to the good or service in the eyes of the consumer". The following eight sources of waste are commonly recognized:

- (1) Overproduction—caused by inflexible or unreliable processes that cause organizations to produce goods before they are required.
- (2) Waiting—caused by inefficient layouts or an inability to match demand with output levels.
- (3) Unnecessary transportation—transporting goods always increases costs and the risk of damage, but it does not necessarily provide value to the final customer.
- (4) Inappropriate process—using overly complex processes, when simpler, more efficient ones would do.
- (5) Unnecessary inventory—caused by uncertainty with regard to quality levels, delivery lead times, and the like.
- (6) Unnecessary/excess motion—caused by poorly designed processes.
- (7) Defects—not only do defects create uncertainty in the process, but also they rob production capacity by creating products or services that require rework or must be scrapped.
- (8) Underutilization of employees—the newest form of waste added to the list. This form of waste recognizes that too often, companies do not fully utilize the skill and decision-making capability of their employees.

The point is to encourage organizations to think critically about the business processes they use to provide products and services, as well as the outcomes of these processes. As far as JIT is concerned, if there is any waste at all, there is possibility for improvement.

The consequence of using the system and process approach in supply chains is the concept of *demand and supply integration* (DSI) (Jüttner et al. 2007). This concept involves coordinating the activities and processes reflective of a firm's customer focus, with the operational, supply-side activities that make demand fulfilment possible. DSI enables firms to maximize relevant revenue streams from customers of choice, that is, those customers or consumer segments whose value requirements best align with the organizations capabilities and generate the most profit (Esper et al. 2010). Esper defined DSI as the "use of organizational processes to balance customer and supply information, so that decisions could be made toward maximizing relevant value creation". Based on organizational learning theories, DSI emphasizes the importance of leveraging market information and business intelligence to gain contextualized knowledge that informs the organizations' strategic decisions and commitments, which enhance the organization's performance. The emphasis of DSI is that both demand market knowledge and supply market knowledge are needed in an integrated fashion in order for firms to facilitate the creation of relevant value. Relevant value reflects an organizational focus on maximizing economic value for both the focal organization and for

customers. By considering market developments from both upstream and downstream forces, organizations are poised to reap the benefits of efficiency-focused operations while simultaneously maintaining relevant levels of effectiveness. The aim of DSI is to leverage knowledge management processes (such as demand and supply capacity planning or sales and operations planning) to facilitate a balance between the needs of customers and the cost and asset commitment required to fulfil the need. This balance results in customer value being created in equal measure with the value that comes back to the organization in the form of economic profit.

A *Demand-driven supply chain (DDSC)* is one method of management which involves building supply chains in response to demand signals (Jüttner et al. 2007; Esper et al. 2010; Monczka et al. 2009). The traditional supply chains use the push concept, while the DDSC uses the pull technique. It gives opportunities to share more information and to collaborate with others in the supply chain. DDSC can be described by a capability model that consist of four levels. The first level is *Reacting*, the second level is *Anticipating*, the third level is *Collaborating* and the last one is *Orchestrating*. The first two levels focus on the internal supply chain while the last two levels concentrate on external relations throughout the *Extended Enterprise*. In a Demand-driven chain or network, a customer activates the material flow by ordering from the retailer, who reorders from the wholesaler, who reorders from the manufacturer, who reorders raw materials from suppliers. In this structure orders flow backwards, up the chain. To create sustainable competitive advantages with DDSN, companies have to do deal with three conditions, so-called ‘3A’: *Alignment* (create shared incentives), *Agility* (respond quickly to short-term change) and *Adaptability* (adjust design of the supply chain). In order to raise demand-driven levels, companies need to undertake a systematic effort that has three main elements:

1. Shortening process lead-time. Overall lead-time is composed of individual cycle-times for multiple processes. This step involves shortening the cycle-time at each step in the critical path processes from the point of purchase to the start of production for the entire supply chain.
2. Adopting flow model economics. Flow model economics encompass low-cost ways to vary mix and volume, similarly to lean manufacturing.
3. Replacing forecasts with demand. This step requires efficient sharing of information up and down the chain. An ideal is for all partners to have access to the level of real-time sales as well as the business rules to react.

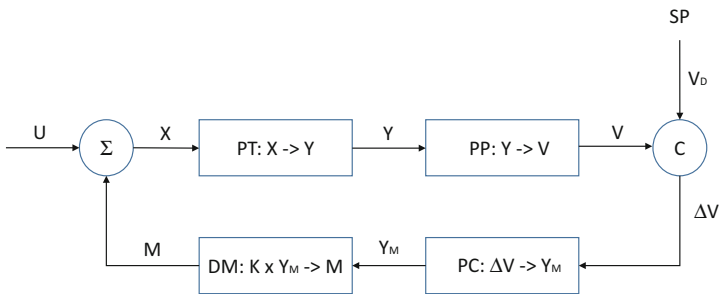
3.3 Attributes of Engineered Systems

3.3.1 Performance-Related Measures

Referring to the models described in formulas (3.4)–(3.8), we propose a general model of a dynamic system— S , which is controlled for performance reasons. Figure 3.7 shows schematically the concept of this model, which is based on the control engineering rules. The main block of the system is a PT-element whose role is to transform the X input into the Y output. The next PP-block is responsible for evaluating the process performance of the S system, assigning the appropriate V_i value for each Y_i output. The next step is to compare the V_i value with the desired value V_D given by the set point SP . The result of the comparison in the form of a ΔV_i error is supplied to the PC-controller in order to calculate the appropriate Y_M value corresponding to the desired value V_D . Then, the decision-maker DM , based on its background knowledge, makes decision M , which should modify the external input U so that the modified internal input X gives—after the transformation—the correct output Y .

For the practical application of the above described model it is necessary to assign appropriate *performance measures* to the parameter V , adequately to the objectives to be achieved by the given process. In accordance with the conclusions from point Sect. 3.1.1 and the rules of the *Statistical Process Control* (SPC 1995), we propose the division of performance measures into three groups: effectiveness measures, efficiency measures and stability measures. Effectiveness and efficiency are usually considered as the primary performance measures for an operating system. They are defined in the following way (Dictionary 2006):

Effectiveness measures how successfully the system achieves its desired outputs. Because this measure involves the subjective reaction of the customer, it is necessary to have a feedback in the system in order to ensure the effective system



System elements: PT – process transformation; PP – process performance assessment; SP – set point; PC – process controller; DM – decision maker; Σ – signal aggregator; C – comparator.
 System parameters: U – external input; X – internal input; Y – output; Y_M – modified output; V – value of performance; V_D – desired value of performance; $\Delta V = V_D - V$; K – background knowledge; M – decision result (input modification).

Fig. 3.7 General model of a dynamic system with the performance control

management. The equivalent of effectiveness for subsystems is *efficacy*. Lars Skyttner defines efficacy as a measure of the extent to which the system contributes to the purposes of a higher-level system of which it may be a subsystem (Skyttner 2008).

Efficiency measures how successfully the inputs have been transformed into outputs. We distinguish two types of efficiency, namely:

- *Technical efficiency*—a measure of the ability of a system (or an organization) to produce the maximum output of acceptable quality with the minimum time, effort, and other inputs,
- *Economic efficiency*—a measure of the ability to produce and distribute its product (or services) at the lowest possible cost.

Stability is a property that characterizes the behaviour of the system over time. It is defined as “the absence of special causes of variation; the property of being in statistical control” (MSA 2010). It refers to both statistical stability of a measurement process and measurement stability over time. Statistical stability implies a predictable, underlying measurement process operating within common cause variation. Measurement stability addresses the necessary conformance to the measurement standard or reference over the operating time of the measurement system.

Table 3.4 shows performance measures divided into groups, types and metrics. Individual performance types will be defined below.

Quality is the ability of a product to perform its functions in the minds of customers, or the ability of service to satisfy customer needs. Quality includes many attributes, however, some of them can be measured objectively, while others can be described only subjectively (e.g. in term of consumer’s perception).

Quantity is generally expressed by the throughput in the description of effectiveness.

Table 3.4 Performance groups, types and metrics examples

Performance group	Performance type	Performance measure
Effectiveness/efficacy	Quality	Value of the product property
	Quantity	Throughput; yield
	Time	Latency; delivery speed and accuracy
	Flexibility	Changeover; product diversity
Efficiency	Productivity	Total productivity
	Profitability	ROA (Return of Assets)
	Inventory cost	Inventory turnover
	Throughput accounting	TAR (Throughput Accounting Ratio)
Stability	Inherent process variation	Variation due to common causes
	Total process variation	Variation due to all causes
	Process capability	Capability index Cp
	Process performance	Performance index Pp

Throughput is the number of such actions executed or results produced per unit of time. This is measured in units of whatever is being produced (cars, motorcycles, I/O samples, memory words, iterations) per unit of time.

Time dimension is usually represented by: latency, delivery speed and delivery reliability.

Latency is the time required to perform some action or to produce some result. Latency is measured in units of time—hours, minutes, seconds, nanoseconds or clock periods.

Delivery speed is understood as a period of time from placing an order until it is delivered.

Delivery accuracy is the characteristic which gives information about the level of trust in the timely realization of the promised delivery.

Flexibility is the ability of a system (or organization) to change as needed to produce or to serve customers. There are many kinds of flexibility, including *changeover flexibility* (the ability to quickly provide a new product or service), *volume flexibility* (the ability to alter the number of products or service flow throughput as needed), and *product diversity flexibility* (the ability to handle a wider range of products or services on request).

Productivity is a basic measure of the production systems efficiency. Its metric is the ratio of the total amount of products produced at a given time to the total amount of resources used to make them (*total productivity*), or to the amount of individual types of resources (e.g. materials, energy etc.) used to make them (*partial productivity*).

Profitability is measured by the ratio of profits made by the system (organization) to: the value of sales (*net profitability*), the value of assets engaged in the production or services (*ROA—Return on Assets*), the value of equity (*ROE—Return on Equity*), or the value of the capital expenditure (*ROI—Return on Investment*).

Inventory cost—the total cost of the material resources accumulation within an operating system. It includes all the transformed resources that are locked up in the system (so-called locked-up capital), such as work in progress, scrap, rejects etc. *Inventory turnover* is the number of times inventory is processed or turned over in a system, or organization, and can be calculated as ratio of cost of goods sold to average inventory value.

Throughput accounting is an approach for short-term decision-making in which all conversion costs are treated as fixed costs. Its metric is the *throughput accounting ratio* (TAR), that can be calculated as a result of dividing the value of return per factory hour by the value of cost per factory hour.

The following four measures are mainly used to describe the *stability of processes* (SPC 1995):

Inherent process variation, which is understood as the portion of process variation due to common causes only. This variation may be calculated from control charts of “average and range” type.

Total process variation, which is understood as the process variation due to both common and special causes. This variation can be calculated based on the standard deviation estimated from a sample or from control charts of “average and standard deviation” type.

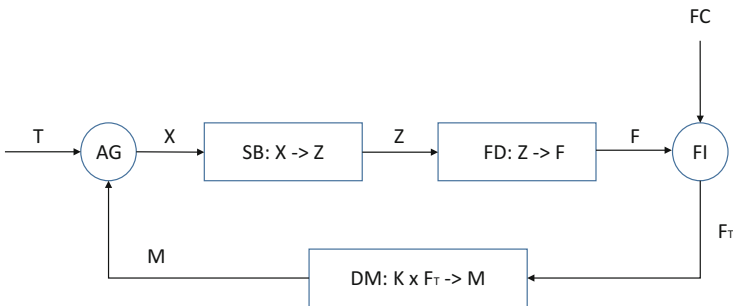
Process capability, which is defined as the 6σ (six standard deviations) range of a process inherent variation, and described by *capability index* C_p . This index can be calculated as the division result of process tolerance width divided by the 6σ range of a process inherent variation.

Process performance, which is defined as the 6σ range of a process total variation, and described by *performance index* P_p . This index can be calculated as the division result of process tolerance width divided by the 6σ range of a process total variation.

3.3.2 Operationality Related Measures

Based on the assumptions from Sect. 3.1.1, we propose a general model of a dynamic system—S, which is controlled for operationality reasons. Figure 3.8 shows schematically the concept of this model, which is based on the control engineering rules. The main block of the system is a SB-element whose role is to transform the input X into the state of system Z. The next FD-block is responsible for the fault detection of the S system, assigning the appropriate faulty state kind F_i for each faulty Z_i state. The next step is FI—fault identification, in which the F_i is compared with the typical faults kinds given by the fault classifier FC. The result of the comparison in the form of a fault category F_C is supplied to the decision-maker DM, who based on his background knowledge K, makes decision M, which should modify the external input T so that the modified internal input X gives, after the transformation, the correct output Z (proper state of the system S).

In practice the correct service is delivered when the system's behaviour allows it to fulfil the required functions, described by the system specification. A *fault* is that part of the system states that may cause a subsequent failure. A *failure* is an event



System elements: SB – system behaviour; FD – fault detection; FC – fault classifier; FI – fault identification; DM – decision maker; AG – aggregator.

System parameters: T – threats (uncontrollable input); X – modified input; Z – system state; F – faulty state; Fr – fault type; K – background knowledge; M – decision result (input modification).

Fig. 3.8 General model of a dynamic system with the operationality control

that occurs when a fault alters the service quality, and the delivered service deviates from a correct service. A system may fail either because it does not comply with the specification, or because the specification did not adequately describe its function. Thus a failure is a transition from correct service to incorrect service, which means that the system does not implement intended function. A transition from incorrect service to correct service is a *service recovery*. The time interval during which incorrect service is delivered is a *service outage*. A system can fail in the different ways, therefore we can distinguish different fault categories and failure modes.

The ability to provide of a service that can justifiably be trusted is called *dependability*, and is used as *a collective term describing the time-related operating quality of a system*. The concept of dependability includes the constituent properties, that can be represented in the form of a ‘dependability tree’, consisting of three levels. Dependability is divided into four main attributes (Bukowski 2016):

- *Availability (AV)*—ability to be in state to perform the required functions under given work conditions, is described by:
 - *Reliability (REL)*—ability to perform the required functions, without failure, for a given time interval, under given work conditions;
 - *Maintainability (MAI)*—ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance;
 - *Maintenance Support Performance (MSP)*—effectiveness of an organization in respect to maintenance support;
- *Safety (SA)*—ability to operate, normally or abnormally, without danger of causing human injury or death and without damage to the system’s environment, it consists of:
 - *Absence of Critical Damages (ACD)*;
 - *Protection of the environment* against the effects of any potential critical damages (*PRO*);
- *Security (SE)*—ability to prevent an unauthorized access to, or handling of system state, can be described by the concurrent existence of:
 - *Confidentiality (CON)*—unavailability to non-enabled persons;
 - *Integrity (INT)*—impossibility of introducing changes into the system by non-enabled persons;
 - *Accessibility for enabled users only (ACC)*;
- *Resilience (RE)*—a collective term describing the ability of a system to absorb and withstand the failure impact, and still continue to operate at acceptable predefined performance level, is described by:
 - *Survivability (SUR)*—capability of a system to fulfil its function, in a timely manner, in the presence of failures (absorbability);
 - *Recoverability (REC)*—capacity of a system to recover from a failure, within the acceptable time and costs limits (restoration);

Table 3.5 Dependability attributes and its metrics

Attributes	Examples of metrics
Availability	Mean availability— $A_m(t_1, t_2)$; mean down time—MDT;
Reliability	Mean failure rate— $\lambda_m(t_1, t_2)$; mean time to failure—MTTF; mean time between failures—MTBF; reliability function— $R(t_1, t_2)$
Maintainability	Mean repair time MRT; mean time to restoration—MTTR
Maintenance support performance	Mean administrative delay—MAD; mean logistic delay—MLD
Safety	Probability that a system will be fully functioning or will fail in a manner that causes no harm in the time period (t_1, t_2)
Security	Probability that a protection subsystem of a main system will be able to prevent an unauthorized access to the system in the time period (t_1, t_2)
Resilience	Probability that a system will be able to fulfil its function in the presence of failures in the time period (t_1, t_2) ; mean time to “bounce back”—MTBB

- *Adaptability (ADA)*—ability to adapt to changed working conditions (flexibility, agility, ability to learn).

This dependability attributes and some examples of its metrics are shown in Table 3.5.

Based on this structure of properties the dependability of a system, for a given time interval (t_1, t_2) , can be described by the model:

$$D(t_1, t_2) = \{AV(t_1, t_2); SA(t_1, t_2); SE(t_1, t_2); RE(t_1, t_2)\} \quad (3.21)$$

This model can be interpreted as follows:

A system's dependability is the collective term, that describes its ability to continuous, safe and secure fulfilment the required functions in a risky environment.

In this approach, dependability can be considered as the opposite of vulnerability, understood in the following way:

Vulnerability is the degree to which a system is affected by a risk source or susceptible to damage, harm or impact.

Vulnerability to a disruptive event is the degree to which a system is affected by a disruptive event. However, the measure of vulnerability can be the disruption impact described by two main indicators: the expected loss of performance, and disruption time.

The model (3.21) become particularly useful at the design stage of complex engineered systems (CES). In situations when insufficient data number does not allow to estimate the statistical measures, the expertise is used to assess the dependability of a CES. An example of the expert-oriented advisory system, that allows for assessment of the degree of background knowledge uncertainty, is shown in Sect. 6.2.

A more detailed analysis of the dependability problem will be made in the Chap. 4, and in particular in Sect. 4.3.

References

- Ackoff RL (1971) Towards a system of systems concepts. *Manage Sci* 17(11):661–671
- Ackoff RL, Magidson J, Addison HJ (2006) *Idealized design: creating an organization's future*. Pearson Education
- Baida Z, Gordijn J, Omelayenko B (2004) A shared service terminology for online service provisioning. In: *The 6th international conference on electronic commerce (ICEC 2004)*
- Barabasi A-L et al (1999) Emergence of scaling in random network. *Science* 286(5439):509–512
- Boulding K. (1956) General system theory—the skeleton of science. *Manage Sci* 2
- Bukowski L (2016) System of systems dependability—theoretical models and applications examples. *Reliab Eng Syst Saf* 151:76–92
- Bukowski L, Feliks J, Majewska K (2016) Logistic system resilience modelling—a dynamic, multiagent, service engineering oriented approach. In: *Risk, Reliability and Safety: Innovating Theory and Practice*. Taylor & Francis Group, A Balkema Book, London, pp 2207–2214
- Cardoso J, Voigt K, Winkler M (2009) Service engineering for the internet of services. In: Filipe J, Cordeiro J (eds) *ICEIS 2008, LNBIP 19*. © Springer, Berlin, Heidelberg, pp 15–27
- Dictionary (2006) *A Dictionary of Business and Management*. Oxford University Press Inc, New York
- Dittes FM (2012) *Komplexität*. Springer Vieweg
- EN ISO 9000 (2015) *Quality management systems—fundamentals and vocabulary*
- EN ISO 9001 (2015) *Quality management systems—requirements*
- ERISS (2016) Tilburg School of Economics and Management, the European Research Institute in Service Science. <http://www.tilburguniversity.nl/eriss/research/service/>
- Esper TL et al (2010) Demand and supply integration: a conceptual framework of value creation through knowledge management. *J Acad Mark Sci* 38(1):5–18
- Eusgeld I, Nan C, Dietz S (2011) System-of-systems approach for interdependent critical infrastructures. *Reliab Eng Syst Saf* 96(6):679–686
- Gharajedaghi J (2006) *System thinking. Managing chaos and complexity*, Elsevier
- Gideon JM, Dagli CH, Miller A (2005) Taxonomy of systems-of-systems. In: *Proceedings CSER 2005*, Mar 23–25, Hoboken, NJ, USA 363
- Jamshidi M (ed) (2009) *System of systems engineering, innovations for the 21st century*. Wiley
- Jüttner U, Christopher M, Baker S (2007) Demand chain management—integrating marketing and supply chain management. *Ind Mark Manage* 36:377–392
- Klir GJ (1969) *An approach to general systems theory*. Van Nostrand Reinhold Co
- Klir GJ (1991) *Facets of systems science*. Plenum NY
- Luzeaux D et al (2011) *Complex system and systems of systems engineering*. ISTE Ltd and John Inc
- Mesarovic MD (1972) Mathematical theory of general systems. In: Klir GJ (ed) *Trends in general system theory*. John Inc
- Mill JS (2002) *A system of logic*. University Press of the Pacific, Honolulu
- Monczka RM, Handfield RB, Giunipero LC, Patterson JL (2009) *Purchasing and supply chain management*. South-Western Cengage Learning
- MSA (2010) *Measurement systems analysis. Reference Manual*
- Newman MEJ (2010) *Networks. An introduction*. Oxford University Press
- Salvendy G, Karwowski W (2010) *Introduction to service engineering*. Wiley, New Jersey
- Sampson SE (2010) A unified service theory. In: Salvendy G, Karwowski W (eds) *Introduction to service engineering*. Wiley, New Jersey

- Sheffi Y (2016) The power of resilience. In: How the best companies manage the unexpected. The MIT Press
- Skyttner L (2008) General systems theory. In: Problems, perspectives, practice. Word Scientific
- Sousa-Poza A, Kovacic S, Keating C (2008) System of systems engineering: an emerging multidiscipline. *Int J Syst Syst Eng* 1:1–17
- SPC (1995) Statistical process control. Reference manual
- Valerdi R et al (2008) A research agenda for system of systems engineering. *Int J Syst Syst Eng* 1:171–88. (Interscience Publisher)
- von Bertalanffy L (1955) General system theory. *Main Curr Mod Thought* 71(75)
- Watts et al (1998) Collective dynamics of ‘small-world’ networks. *Nature* 393:440–442
- Weinberg G (1975) An introduction to general systems thinking. NY Wiley
- What is Delivery Management? (2018) <https://it.toolbox.com/blogs/deliverydr/what-is-delivery-management-070606>
- Zio E (2007) From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructure. *Int J Crit Infrastruct* 3(3/4):488–508

Chapter 4

Designing Complex Engineered Systems for the Risky Environment



It is not the strongest of the species that survives, nor the most intelligent that survives.

It is the one that is the most adaptable to change.

Charles Darwin.

4.1 Creating Reliable Infrastructures

4.1.1 System of Systems Engineering

Since the 1970s the engineered and social systems have changed into large-scaled and highly sophisticated complex organizations. These systems have restrictions on information structure and critical sensitivity to risks (Keating 2005). In reply to the emerging features and increased demands for control, the paradigm of Large-Scale Systems (LSS) has appeared in system theory. A system was considered as large-scale, with three general attributes: ability to decompose, centrality for geographical distribution and complexity.

System of Systems (SoS) is a natural extension of LSS in systems engineering. The paradigm 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 particular task, assessing uncertain environment influence during SoS operation, and ensuring operative compatibility (interoperability) between SoS components.

The distinctions between SoS and LSS have been declared initially by (Maier 1998), and consist in the following general properties and characteristics:

- Operational independence of the components in a SoS,
- Evolutionary development (necessary changes in a SoS can be made, new functions added, removing or updating existing ones). SoS undergoes persistent evolution, in contrast to multi-step non-cyclic irreversible design of LSS,
- Emergent, suddenly changing and non-predictable behaviour (Jamshidi 2008),

- Spatial distribution (Eisner 1993) denoted SoS as large geographically dispersed complexes),
- Guaranteed interoperability between two or more systems and components to exchange information and operate independently by utilizing available information (IEEE 1990)—only a SoS is able to interoperate its component systems,
- Complementarity (each system should complement the other members within SoS). The multiple perspectives ensure robust approach and design (Keating 2005),
- Guaranteed integrity and on-line membership optimization,
- Holism (the overall entity is more informative than the sum of its parts).

The comparison between LSS and SoS modelling processes shows significant differences. The typical LSS modelling process evolves from top of the hierarchy to the bottom. Whereas, during the SoS modelling the appropriate development is oriented ‘from bottom to top’ of the system. The first descriptive characteristic for the notion of the System of Systems Engineering (SoSE) is made primarily by (Keating et al. 2003; Jamshidi 2005), but actually SoSE is understood as “an integrated approach to upgrade existing systems to newer, more powerful and improved systems for command, control, communications, computer hardware intelligence, surveillance, reconnaissance and innovative logistic support” (Tzanev 2013).

The general distinctions between SE and SoSE refer to the following points (Sage and Cuppan 2001):

- Significantly expanded system of systems requirements for ranking level of strictness and rigour,
- Centralized in substance (although distributed in space) control structure in LSS versus decentralized control and component disposition of SoS,
- LLS with well-defined final states, fixed resources, clearly planned schedules, technical baselines and homogenous structure versus SoS with vaguely defined end states, periodical variations of supply and delivery, as well as heterogeneous structure of equipment.

The most problems typical for system of systems engineering do not have a precise cause-and-effect relationship and they are not reducible to the models required for application of analytical methods, which can produce optimal solutions. Optimisation in the mathematical sense is not possible and cannot be used for the solution of these system problems (de Weck et al. 2011; Hester 2012). The main problems of the complex systems are consistent with Rittel and Webber’s (1973) ‘wicked problems’ (understood as problems that are intractable with current levels of thinking, decision, action, and interpretation), and with Ackoff’s modification of this concept (Ackoff et al. 2006), namely a notion of ‘mess’ (defined as interrelated sets of problems that are not well formulated, understood, or easily resolved). This ‘problem space’ is marked by difficulties encountered across the holistic range of tangled technical, organisational, managerial, human, social, information, political,

and policy issues, and represents the ‘new normal’ for complex systems (Keating and Katina 2016).

The SoSE requirements are summarized in ensuring compatibility and interoperability of the system components with highest levels of operational efficiency. Three perspective directions are examined as a proof of the observed field fragmentation (DoD 2008): military, industrial and academic developments. Military perspective is issued by the US Department of Defense (DoD) and focused on the interoperability of technical command and control systems. The set of individual systems requires integration of the separate technical components in an overall SoS. Industrial perspective possesses a more robust view of SoSE and considers a manufacturing company as a SoS, existing well beyond the technology. The central problem of the industrial perspective trends is occupied by the system architecture, that is the dominant paradigm in SE (Maier 1998). Academic perspective demonstrates potential for future rigorous development in theoretical aspects. The academic contributions are based on the following commonly accepted assumptions:

- SoS provides services, behaviour or performance, impossible to meet by any single system,
- Each subsystem operates independently with the aim to realize its own goals, often different by that of SoS,
- A SoS is constituted by multiple subsystems (e.g. LSSs), functioning in a common mission,
- Intended and random chains of events are emerging as a result of the interactions between the subsystems, jointed in a SoS, and their environment.

4.1.2 Engineered System of Systems and Its Main Attributes

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 behaviour and functioning locally when facing any change of their environment (Ackoff 1971; Boardman and Sauser 2006; Carney et al. 2005; Jamshidi 2011; Maier 1998). It is admitted that the SoS Engineering (SoSE) activities focus 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 in order to fulfil the SoS objectives.

The process of purposefully 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 (in alphabetical

order): extensibility, flexibility, integrateability, interoperability, interchangeability, modularity, portability and replaceability.

Extensibility of an open system is understood as the 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 needs, can be reconfigured and modified to changing situations.

Integrateability of a given system means that it is able to form, coordinate, or incorporate into a larger, functioning or unified whole.

Interoperability seems to be the most important attribute of ESoS, therefore, it will be discussed in detail later.

Interchangeability means that a given system or a part of it can be replaced with another one without losing the basic system properties.

Modularity of a given system means that a given system (usually in order to improve its maintainability) is built of functional blocks, separating the system's capacities into modules.

Portability is the ability to be readily moved from one environment to another.

Replaceability is understood as the ability of one system, component or person to take the place of another, especially as a substitute or successor.

Interoperability is required to coordinate and make such large multi-disciplinary and heterogeneous combination of subsystems efficient. Therefore, interoperability has to be fully considered when the chosen subsystems are assembled for a given period of time during which they will have to work together, share flows of data and resources in order to build their SoS.

We understand interoperability as the ability of connected, autonomous, flexible coupled and usually heterogeneous systems to cooperate and to exchange flows of data, services, material and energy to and/or from other systems, while continuing their own way of operation.

The autonomy of a subsystem (e.g. the ability to continue operations and make decisions, in order to ensure its own mission independently of other subsystems) is consistent with the expected managerial independency of the subsystems. The reversibility of a relation between two subsystems that allows a subsystem to achieve its mission, after breaking an alliance with other subsystems composing the same SoS, is coherent with the requested operational independency of the subsystems (Billaud et al. 2015). The subsystems are flexibly coupled, and this kind of coupling enhances the connectivity which characterizes a SoS, where subsystems are capable of building links among their interfaces and destroying them dynamically (SIoT 2006). On the other hand, this flexibility enhances the evolutionary development of the SoS (Maier 1998) when it becomes possible to easily remove, modify or add subsystems from the SoS. The heterogeneity of the subsystems is essential for the SoS since it can only achieve its global objective by leveraging the diversity of its subsystems (SIoT 2006). Thus, maintaining a sufficient level of interoperability of each subsystem helps the preservation of the most important SoS characteristics (constituent subsystems autonomy, enriched connectivity and

commitment to diversity of subsystems) and the SoS behaviour. Real SoS passes through various stages in its life cycle during which these characteristics may evolve but have to be maintained in an acceptable range.

The basic interoperability requirements include the subsystems *autonomy* and *compatibility*. The compatibility refers to the interfaces imposed by the interactions between the subsystems. Interfaces can be technological, organizational or logical at different levels of abstraction. Imposing standards interfaces or human-machine interfaces and common integration mechanisms are not always the sufficient solution in dynamic environment of SoS (Kasunic 2004; Panetto 2006). The *autonomy* means that each subsystem must effectively respect the expected objectives, stakeholders' requirements and constraints defined for the SoS (e.g. cost, delay, quality) but meanwhile, it should respect its own requirements. During the operational phase of the SoS, subsystems' interoperation concerns the ability of a collection of subsystems to share or exchange specified information/energy/material in order to achieve a specified purpose/mission in a given context. In the dissolution phase of the SoS, the inter subsystems' relations (reversibility) is an important interoperability requirement. For instance, once a set of subsystems break the alliance with each other, each subsystem must be able to return to a state in which it reaches at least its original level of performance while executing its usual operations and consequently respecting its own requirements (Billaud et al. 2015). Interoperability requirements are not the same for all systems, but they can vary from one SoS type to another.

Generally *compatibility* is necessary to harmonize subsystems in order to be ready for collaboration. However, compatibility focuses on a static point of view of the collaboration and remains insufficient to determine if the subsystems are interoperable during the SoS life cycle. It is also essential to consider the evolution of the context and the situation of each subsystem. Therefore, an adequate set of indicators is required to analyse the impact of the compatibility between the subsystems on the performance of the SoS. Usually they are divided into subgroups according to the kind of compatibility (Billaud et al. 2015):

- Organizational and conceptual compatibility indicators: syntax (is the information to be exchanged is expressed with the same syntax?), preparedness (is the data are well defined and documented?), understanding (is communication and shared information rate proper?), command style (are authorities and their responsibilities are clearly defined?) and trust.
- Technical compatibility indicators: Common Operating Environments (COE), standard procedures and training, standard complaint, basic data format (Information exchange is restricted to homogeneous data exchange), media format, applications, security profile (a security profile contains information that governs at what security level a system may operate), media exchange procedures, system services, data, heterogeneous information (contain more than one data format) and information space.

- Operational and behavioural compatibility indicators: compatibility with prior experience, compatibility with existing work practices and compatibility with preferred work style.
- Functional compatibility can be described by response and execution time.

Interoperation is the ability of a set of communicating systems to share or exchange specified flows (e.g. data, information, energy, material or services) in order to achieve a specified purpose in a given context. It is measured through a set of indicators which are adequate to a specific types of telecommunication SoS. These indicators can be applied to any kind of SoS if the flows between subsystems constitute: data, information, material or energy. The most important interoperation indicators are as following (Billaud et al. 2015):

- Time of interoperation—the time corresponding to the duration between the moment when information is requested and the moment when the requested information is used;
- Quality of interoperation—it takes into consideration three kinds of quality:
 - the quality of exchange (it draws up if the exchange is correctly performed),
 - the quality of use (it represents the number of information received by a partner in comparison with the number of information requested) and,
 - the quality of conformity (to what extent it corresponds to the exploitation need of the information);
- Capacity—is the rate at which data may be passed over time;
- System overload—when more data must be exchanged than the system is able to transmit;
- Under-utilization—when the system data rate load is less than its full capacity but messages are waiting in queues to be transmitted;
- Under-capacity—when messages remain in queues and the system data rate is at the maximum;
- Data latency—is the elapsed time from the transmission to the reception.

4.1.3 Architecting Reliable ESoS

According to the ESoS definition from Sect. 4.1.2, 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 role in relation to all subsystems. Thus, the design, instalment, operation and transformation of metasystem, which operates as an integrated complex system to perform new desirable results, 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.

Effective architecting of reliable ESoS requires a purposeful, holistic, and comprehensive approach to deal with complex systems and their inherent problems. This area of SoSE has been previously identified as an emerging field dedicated to guiding design, execution, and evolution of the essential metasytem functions that are required to sustain and evolve system performance (Keating et al. 2014). 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*. Each of these elements and their particular role are described below.

The first essential element is the *metasystem construct*. The metasystem construct brings several important considerations, including (Keating and Katina 2016):

- the metasystem operates at a logical level beyond the system/subsystems/entities that it must integrate,
- the metasystem construct 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 organisation),
- the metasystem 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,
- the metasystem 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 still continue its existence,
- a metasystem can be purposefully designed, executed, and maintained, or left to its own (self-organising) unstructured development.

The metasystem construct is a cornerstone 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 of internal system flow and external environmental turbulence. The primary function of control by the metasystem is to provide the minimal constraint necessary to ensure continued system performance and behaviour, while maximising autonomy of governed entities. In this sense of control, the maximum level of autonomy is reserved for governed subsystems. This can be achieved by implementing the constraints necessary to provide sufficient stability that ensures system performance levels can be maintained. The achievement of this stability is accomplished through the metasystem’s ability to provide sufficient regulatory capacity to mitigate the turbulence generated from the environment as well as from the flow generated internally to the larger system. This regulatory capacity seeks to provide the highest degree of autonomy possible to the subsystems being governed. The metasystem provides only as much control as it is

necessary to integrate the subsystems to support the larger purpose (e.g. performance, behaviour, etc.) expected from the system. Control generated by the metasystem is achieved in conjunction with three other 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, actions, 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 in order 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 subfunctions. The metasystem functions find their genesis in the works of Beer's (1979, 1984, 1985). The interrelated governance functions must be performed if a system is to remain viable (continue to exist) under conditions of internal flow and external turbulence. These main functions are as follows (Keating and Katina 2016):

1. Policy and identity—focused on overall steering and trajectory for the system. Maintains identity and defines the balance between current and future focus from two perspectives:
 - System perspective—focused on the specific system context within which the metasystem is embedded. Context is the set of circumstances, factors, conditions, patterns, or trends that enable or constrain execution of the system.
 - Strategic perspective—focused on oversight of the system performance indicators at a strategic level, identifying system level performance that meets, exceeds, or fails to meet established performance expectations.
2. System development—maintains the models of the current and future system, concentrating on the long range development of the system to ensure future viability.
 - Environmental monitoring—designs, deploys, and monitors sensing of the environment for trends, patterns, or events with implications for both present and future system viability.
 - Learning and transformation—focused on facilitation of learning based on correction of design errors in the metasystem functions and communication channels and planning for transformation of the metasystem.

3. System operations—focused on the current execution of the metasystem to ensure that the overall system maintains established performance levels.
 - Operational performance—monitors system performance to identify and assess aberrant conditions, exceeded thresholds, or anomalies.
4. Information and communications—designs, establishes, and maintains the flow of information through communication channels, and consistent interpretation of exchanges necessary to execute metasystem functions.

The main metasystem functions do not operate independent of one another, but are interrelated. The execution of the functions as well as communication channels determines the level of governance effectiveness and finally system performance.

The third fundamental element of this approach is the set of *communication channels*. These channels provide for the flow of information and consistency in interpretation for exchanges within the metasystem and between the metasystem and external entities. The ten communication channels are adapted from the work of Beer (1979, 1984, 1985) and extensions of Keating and Morin (2001). Table 4.1 provides a concise listing of the communication channels, their primary metasystem function responsibility, and the particular role they play in metasystem execution.

The fourth essential foundational element of architecting reliable ESoS rests in the *relationship between the metasystem and that which is governed* (subsystems) by the metasystem. Thus, governance permits establishment and maintenance of system coherence (its identity) and cohesion (its unity). At the basic level, the metasystem keeps the system from either collapsing from external pressures or flying apart from internal pressures. It is what keeps the system from separating in the face of increasing complexity.

The development process of ESoS architecture can be divided into three stages (Keating and Katina 2016). The first stage—*initialisation*—is directed to providing an initial understanding of the situation and system of interest. This understanding encompasses the nature and structure of the established system of interest, and is called framing. The framing serves to articulate the current state of the system under exploration. The second step of initialisation is the context within which the embedded system of interest. The system is embedded in the context, which represents the circumstances, factors, patterns, or trends that constrain the system. With these two elements completed, a rigorous understanding of the system and its context is established.

Completion of the initialisation stage provides a foundation for the second step of development, namely *Governance Readiness Level Assessment (GRLA)*. GRLA is targeted at the analysis of the variety constructed from the initialisation stage. The nature of this stage suggests an interpretative examination of the initialisation stage seeking an answer to the question: What do the different artefacts from initialization suggest for the state of system governance and implications for development? This requires a deep and broad introspection by the designers, owners, operators as well as performers of the system. Ultimately, the results of this stage provide an indication of two critical elements. First, appreciation of the current state within a

Table 4.1 Communication channels of the metasystem (based on Keating and Katina 2016)

Function	Subfunctions	Description of the function's role
1. Policy and identity (PI)	1.1 Command	Provides non-negotiable direction to the metasystem and governed systems
	1.2 Control	Provides for examination of system decisions, actions, and interpretations for consistency with system purpose and identity
	1.3 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
2. System development (SD)	2.1 Environmental monitoring	Provides design for sensing to monitor critical aspects of the external environment and identifies environmental patterns, activities, or events with system implications
	2.2 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
3. System operations (SO)	3.1 Resource management	Determines and allocates the resources (manpower, material, money, methods, time, information, support) to governed systems and defines performance levels (e.g. productivity), responsibilities, and accountability for governed systems
	3.2 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
	3.3 Audit	Provides routine and sporadic feedback concerning operational performance as well as investigation and reporting on problematic performance issues within the system
4. Information and communication (IC)	4.1 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
	4.2 Informing	Provides for flow and access to routine information within the metasystem or between the metasystem and governed systems

classification scheme for governance. Second, based on this state classification, identification of the general classes of feasible ESoS development activities might

be undertaken with a reasonable chance of success. Thus, by understanding the readiness level of the metasystem, the broad range of activities that might be undertaken can be prioritised along two dimensions: potential impact for addressing system governance deficiencies and feasibility of success for the activity given the readiness level of governance.

The third stage of development is entitled *governance development*. The two prior stages were passive and not directed to initiation of activities to enhance the state of system. The third stage identifies the feasible activities that will be engaged in support of metasystem development. However, there are three important aspects to this stage. First, feasibility is a function of the state and the corresponding levels of development activities. Second, includes the prioritisation of activities based on the overall condition of governance. Therefore, more informed decisions can be made with respect to the highest payoff development investments. Third, activities are targeted to make either contextual improvements or metasystem governance improvements. This continuous development should be implemented in the form of an evolutionary process. In practice the execution of these steps is usually emergent and overlapping.

The Fig. 4.1 shows the general functional structure of an Engineered System of Systems. The function and subfunction notation is based on the symbols from Table 4.1. The multilevel functional structure of subsystems interconnected with the metasystem is shown in Fig. 4.2. The example shown in this figure concerns a four-level structure composed of modules, components and elements, interconnected by mapping relations. Individual parts of the entire structure may also be connected to some parts of other subsystems (these connections are symbolized by dashed lines).

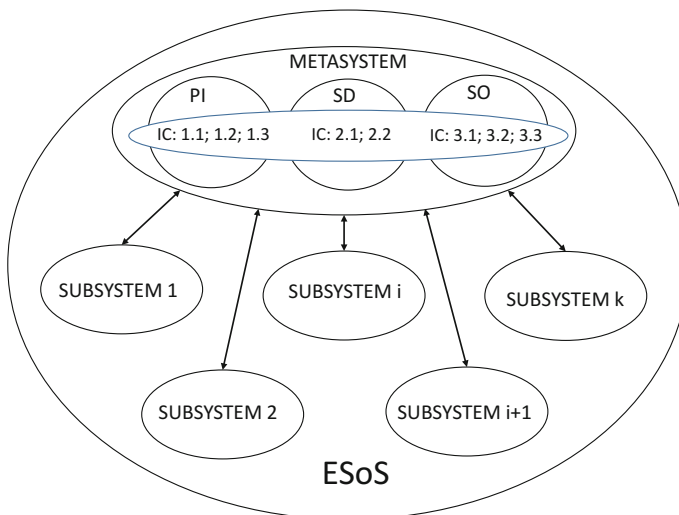


Fig. 4.1 The general functional structure of an engineered system of systems

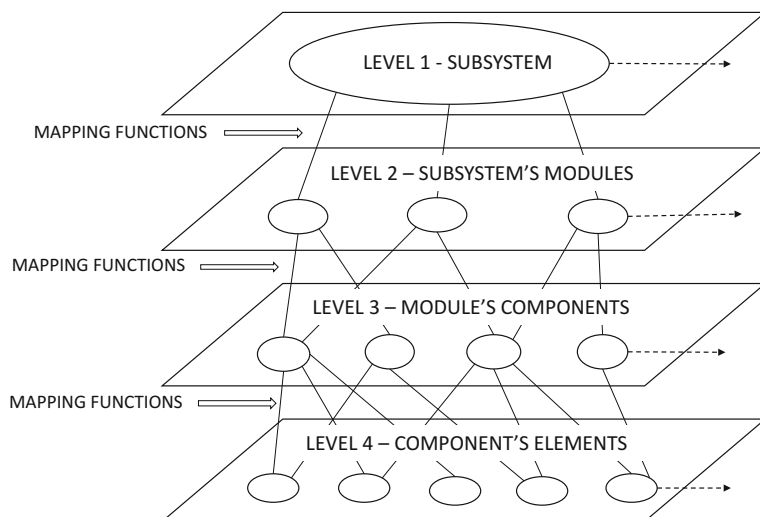


Fig. 4.2 The multilevel functional structure of an engineered system of systems—an example for four level hierarchy

4.1.4 Building High Reliability Organisations

A High Reliability Organisation (HRO) is an organisation which has succeeded in avoiding catastrophes in an environment where normal accidents can be expected due to risk factors and high complexity. This concept is based on the *Normal Accident Theory (NAT)* developed by Charles Perrow in 1984 and its main premise is that accidents are inevitable in complex organisations that operate high-risk technologies. Perrow argued that there are certain defining characteristics, which make the occurrence of accidents in complex, high hazard organisations 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, equipment, procedures), whilst interactive complexity refers to the extent to which the interactions among the system's components are unpredictable and invisible. Therefore, high-risk organisations are those that operate systems, which are very complex and can interact in unexpected ways. Consequently, because of interdependency, a failure that occurs in one part of the system can quickly spread 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).

Doubtless the Normal Accident Theory has advanced the understanding of system characteristics that increase the likelihood of catastrophic events, but it has also a number of weaknesses and imperfections. Some experts (e.g. Hopkins 2007) argues that the central concepts of NAT, namely coupling and complexity, are poorly defined and the theory itself can only explain a small number of accidents

because it applies to very specific types of organisations. Furthermore, the theory provides a pessimistic view regarding accidents in complex systems and fails to offer suggestions as to how the risk of accidents may be reduced.

In order to remove the NAT defects researchers at the University of California, Berkeley, defined concept of High Reliability Organisation (HRO) in terms of an organisation's ability to sustain almost error-free performance over long time periods (e.g. Roberts 1990). This definition, has been criticised as being too general and helpless in terms of identifying an HRO. Hopkins (2007) noted that several organisations could fail catastrophically every minute of every day and would still be identified as 'high reliability' because they still manage to succeed much more often than they fail.

Traditionally, HRO researchers have relied on accident statistics as evidence that an organisation meets the 'high reliability' criterion of almost error-free performance. However, these statistics have been criticised as lacking objectivity and confounding reliability with safety. Roberts and Rousseau (1989) identified several characteristics that, they argued, distinguish HROs from other kinds of organisations, including:

- Hyper complexity and tight coupling—the organisation is characterised by a variety of components and systems, which are interdependent and its processes are unpredictable and difficult to interrupt;
- Extreme hierarchical differentiation—multiple levels, each with its own elaborate control and regulating mechanisms;
- Large numbers of decision-makers in complex communication networks—characterized by redundancy in control and information systems;
- Degree of accountability that does not exist in most organizations—substandard performance or deviations from standard procedures meet with severe adverse consequences;
- Compressed time factors—cycles of major activities are measured in seconds.
- More than one critical outcome that must happen simultaneously.

Weick and Sutcliffe (2007) identified main characteristics that they defined as 'reliability-enhancing'. The first is defined as preoccupation with potential errors and failures. Incidents and near misses are seen as indicators of a system's 'health and reliability'. For this reason, the reporting of near misses and errors is viewed as learning opportunity and a means of obtaining a realistic picture of operations. Then, near misses are thoroughly analysed because they are seen as opportunities to improve processes.

The second reliability-enhancing characteristic is defined as aversion to simplify and focus on HROs' ability to collect, analyse and prioritise all warning signs that something may be wrong and avoid making any assumptions regarding the causes of failure (Weick and Sutcliffe 2007). For example, HROs assume that failures are systemic, rather than localised in nature, and could potentially lead to a broader causal chain of events with potential catastrophic consequences.

Resilience is the next reliability-enhancing characteristic and is concerned with the ability of HROs to effectively anticipate errors as well as to cope with and bounce back from errors and ‘unexpected events’ (Weick and Sutcliffe 2007). This characteristic exemplifies HROs’ commitment to learning from past experience and errors both from within the organisation and from other industries.

Deference to expertise is the final HRO characteristic proposed by Weick and Sutcliffe (2007). For the period of normal operations, HROs are characterised by a hierarchical structure with clearly defined roles and responsibilities and lines of reporting so that everyone knows who is responsible for what. However, in emergencies, this structure exists no more, and decision-making is deferred to individuals with the expert knowledge to deal with a specific problem, irrespective of their status within the organisational hierarchy.

Roberts and Bea (2001) identified three characteristics that organisations can implement to enhance their reliability:

- Seek to know what we do not know—investment of resources to train and re-train staff to enhance technical competence and enable them to anticipate and respond appropriately to unexpected events. Analysing accidents and near misses to identify the types of accidents that happen in the organisation and target the aspects of the system that require redundancies.
- Balance efficiency with reliability—HROs use incentive schemes to balance safety with profits and enable employees to make decisions that are safe in the short-term and profitable in the long perspective.
- Communicate the broad perspective—HROs should have effective communication channels allowing quick expertise in emergencies and communicate the ‘big picture’ to everyone. It also allows developing well-defined procedures for both normal and emergency situations with well-known decision rules.

As it appears from the above the HRO researchers have described several characteristics and processes that enable organisation to achieve their good safety record and sustain a reliable performance over long time periods. The descriptions capture HROs’ ability to collect, analyse and synthesise information about the ‘bigger picture’ of current operations in such a way that enables them to effectively contain and prevent potential future failures. Hopkins (2007) argues that HROs represent an perfect organisation and real organisations can exhibit varying degrees of reliability-enhancing characteristics. Therefore, there is a justified need to develop new measures that would enable organisations to assess the extent to which they possess ‘reliability-seeking’ characteristics.

The concept of HRO reinforce a distinct set of requirements and behavioural norms that do not commonly exist in other organisations. Koch (1993) developed a measure in order to master the reliability-seeking nature of organisations and that could be generalised to different industries. He proposed two measures: the first was a longer 37-item scale which tapped into culture of reliability-seeking organisations, and the second, with the scale consisting of 25 items which aimed at distinguishing

reliability-seeking organisations from other organisations. The key factors which were captured by the scales included:

- Accountability and responsibility—the degree in which each person of an organisation is responsible for decisions in preventing accidents and ensuring operational safety;
- Interaction and communication—the extent to which knowledge of events flows upward in the organisational hierarchy;
- Adaptiveness and responsiveness
 - the extent to which organisations are able to adapt or recover from unexpected events, and
 - the ability to change from ‘low to high-tempo operations’ (i.e. immediate decision-making in emergencies);
- Threats and hazard awareness—the extent to which organisations are aware and can anticipate dangerous situations and take appropriate action;
- Inquisitiveness and search for detail—the abilities of individual employees to ask questions and to be careful in safety-critical situations;
- Maturity—the extent to which organisations cannot tolerate self-centred, risky behaviour.
- Training and socialisation—the extent to which the organisations’ training procedures and practices capture safety-related values and behaviours among organisational members.

Weick and Sutcliffe (2007) developed a set of measures to enable organisations an assessment of their tendencies toward mindfulness or lack thereof. The measures also capture the five core characteristics of HROs that include preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience and deference to expertise. Authors argue that these audits enable organisations to assess their practices and use the findings to diagnose potential areas that require improvement. For practical applications Vogus and Sutcliffe (2007a, b) developed and validated the Mindfulness Organising Scale in hospital nursing units, which captures the extent to which an organisation demonstrates the abovementioned HRO principles.

There have been several attempts to apply HRO concept in other different contexts. The research by Madsen et al. (2006) highlighted the importance of leadership in implementing and sustaining HRO processes. It was shown that in the absence of leaders that are promoting and championing high reliability processes, the organisation returns to its ‘normal’ way of operation. The importance of effective leadership is also acknowledged by Frankel et al. (2006) who argued that leaders drive the values, behaviours and culture within an organisation and that leadership engagement is one of the key components for enhancing reliability and safety in every organisation.

However, some HRO principles can be ineffective or counter-productive in certain contexts. Tamuz and Harrison (2006) provide an example that excessive

reliance on double-checking may undermine safety critical tasks by breeding a culture of complacency or a sense of diffusion of responsibility—e.g. personnel may neglect important safety checks because they rely on others to duplicate their efforts. The authors caution that the principles and practices that emerged from high reliability theory and normal accident theory should be used as ‘... frames and not as blueprints’ and ‘need to be tested empirically—both through research and through action ...’.

HRO characteristics are often discussed in the context of major incidents and are used to highlight the operational safety standards that organisations should try to emulate. The MIBB report (2008) recommended that the following factors should be addressed to achieve a high reliability organisation:

- A clear 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 procedure design and alarm systems;
- Providing appropriate personnel and shift work arrangements to control major accident hazards;
- Providing appropriate training, experience and competence assurance systems for staff engaging in safety-critical activities;
- Auditing and operational monitoring of contractors’ abilities to supply and maintain high integrity equipment;
- Providing appropriate 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 standardised procedures for key maintenance, testing and operational activities;
- Ensuring that management of change is addressed effectively and includes organisational, procedural and equipment changes.

Another regulatory document published by the Norwegian Petroleum Safety Authority (PSA 2004), the independent regulatory body under the Ministry of Labour and Government Administration, underlines the importance for organisations to have a positive health, safety and environment culture. In particular, the Norwegian PSA recommends that organisations should work towards developing and implementing the following characteristics:

- A reporting culture characterised by good reporting systems and a climate of trust within the organisation—the aim should be to learn from previous incidents and not to attribute blame;
- Reactions to mistakes should be proportionate to the nature and consequences of mistakes and there is a system of rewards and sanctions in place that is perceived as fair and constructive;

- A learning culture whereby information is communicated and shared effectively both horizontally (across different departments or shifts) and vertically (across hierarchical levels within the organisation) but also with customers and sub-contractors;
- A flexible culture that adapts successfully to external demands without compromising safety.

It is also recommended that a combination of qualitative (participant observation, use of documents such as reports, workshops) and quantitative methods (questionnaire-based surveys, structured interviews, injury statistics) should be used to identify and diagnose an organisation's existing health, safety and environment culture (PSA 2004). The importance of management in reducing major accident risks and gathering knowledge from prior incidents is cited as one of the top priorities. In particular, the report emphasises the important role that leaders play in keeping track of the weaknesses in organisational operations, integrating information across different parts of the business, as well as learning from previous errors and applying that knowledge to improve risk management. Leaders are seen as playing a key role in the management of major accident hazards (PSA 2010).

In summary, research in HROs has revealed a number of important processes that play an essential role in the safety performance of these organisations. However, this concept has also raised a number of important questions, predominantly regarding the transferability and underlying mechanisms of HRO processes, as well as their financial justification (Lekka 2011). Table 4.2 shows the main features and processes characteristic for High Reliability Organisation.

Table 4.2 Main features and processes characteristic for high reliability organisation (based on Lekka 2011)

Features	Description
Typical attributes of organisation	• 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 (decentralised) organisational structures, • Investment in training and technical competence, • Well-defined procedures for all possible unexpected events

(continued)

Table 4.2 (continued)

Features	Description
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 organisation • Open communication of accident investigation outcomes, • Updating procedures in line with the organisational 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

4.2 Assurance Process Continuity

4.2.1 *From High Reliable Organisation Concept to Resilience Engineering Approach*

From the safety perspective the resilience engineering approach overlaps with the HRO concept because both approaches strongly emphasize the need to develop and implement their own safety strategy in each organization (e.g. Costella et al. 2009). Resilience engineering has been applied in several ‘dangerous’ areas, such as in aviation, petrochemical and nuclear power industries and involves helping organisations to both avoid failures and be able to recover quickly once these have occurred. Wildavsky (Weick et al. 1999) defined *resilience as the ability to ‘cope with unanticipated dangers after they have become manifest, learning to bounce back’*. Reason (2000, 2005), Wreathall (2006) and Costella et al. (2009) claim that resilience may be ‘engineered’ by incorporating the following characteristics and processes:

- **Safety culture.** There is an open accident and near miss reporting system within the organisation, and individuals are supported and able to suspend work on safety grounds without fear of being penalised for their decisions (a ‘no blame’ approach to mistakes). However, in developing a safety culture a distinction must be made between unacceptable or blameworthy behaviour that requires disciplinary action and other types of behaviour (such as necessary violations arising from inadequacies in the equipment or workplace which make compliance with procedures unfeasible) (Reason 2000, 2005). The development of this type of culture requires a balance between supporting the reporting of incidents and near misses and not tolerating unacceptable behaviours (e.g. Wreathall 2006).
- **Learning culture.** The organisation learns from experience by systematically gathering and analysing near misses and incidents as well as encouraging the reporting of incidents. Costella et al. (2009) argued that organisations can also learn from normal working practices and disseminating and sharing best practice (focusing on how procedures are implemented during normal working practices can help identify any gaps between how managers think that procedures should be used and how they are actually applied by front line staff).
- **Management commitment.** Management balances the pressures of production with safety and management behaviour (including allocation of resources) and sends the message that safety is even more important than other business objectives.
- **Increased flexibility.** Systems should be designed in a way that support, rather than constrain, individuals in carrying out their jobs (employees have the discretion to make decisions when necessary without having to await for management instructions).
- **Preparedness.** The organisation should be proactive in its safety management and be able to anticipate all potential problems, changes, threats and hazards.
- **Transparency.** The organisation should collect and analyse information that enables the identification of weaknesses in its defences. This is in line with the Reason’s (2005) concept of an informed culture whereby the organisation has an understanding of both the hazards that it faces and the adequacy of its defences to control them.
- **Redundancy.** The organization should have resources, which may take the form of either additional staff or time to respond to emergencies, are crucial to enabling organisations to respond to unexpected events.

Provera et al. (2008) argued that a safety culture is essential in promoting both organisational learning and highly reliable operations. They carried out a series of semi-structured interviews in order to identify and compare the attitudes towards blame in HROs (e.g. commercial airlines) and non-HROs (e.g. retail banks). The authors found that a safety culture was characterised by: rewards for the reporting of near misses and accidents, an absence of blame and fear of punishment, debriefing processes whereby individuals involved in incidents actively participated in the investigation process, and outcomes of the investigation process were followed up

through the development of corrective actions that were communicated to all staff. Provera et al. (2008) claim that a safety culture encourages a systemic view of errors and failures rather than ‘blame the operator’ explanations that are typical in traditional organisations, as well as identified several barriers to the development of a this culture in traditional organisations, namely:

- Costly and time consuming—implementing a safety culture requires organisations to invest time and resources in order to re-visit their operational and communication procedures.
- Cultural constraints—people tend to resolve problems with their supervisors or colleagues rather than report them, which limits open communication and learning from mistakes.

In summary, the resilience engineering perspective shares much in common with the HRO approach and offers principles that can be implemented by organisations to improve their reliability and safety performance. However, resilience engineering (RE) differs from HRO primarily because the main goal of RE is to maintain the continuity of production and service processes. This approach is particularly important in complex systems such as critical infrastructure and global supply networks. Therefore, in the further part of the work a more detailed overview of the concepts regarding the application of RE in different disciplines of knowledge and practical applications will be made.

4.2.2 Resilience Science—Transdisciplinary Perspective

Traditionally, the term resilience means the tendency or ability to spring back, and thus the ability of a body to recover its normal size and shape after being pushed or pulled out of shape, and generally any ability to recover to normality after a disturbance. It means being able to withstand shocks and deviations from the intended state and go back to a desirable or acceptable, state. A general definition specifies *resilience as the ability to deliver, maintain and improve service when facing disturbances (e.g. threats and evolutionary changes)*.

A concern in the resilience engineering literature is that measures of disturbances outcomes may lack predictive power: success in the past is no guarantee of success in the future. Thus, a search for leading indicators that can be used to assess future resilience is difficult because of the multidimensionality of resilience. Westrum (2006) writes: ‘Resilience is a family of related ideas, not a single thing. The various situations that we have sketched offer different levels of challenge, and may well be met by different organizational mechanisms. A resilient organization under Situation I will not necessarily be resilient under Situation II (these situations are defined as having different degrees of predictability). Similarly, because an organization is good at recovery, this does not mean that the organization is good at foresight’.

Although the idea of resilience have been introduced relatively recently, it have already been examined in many serious studies, both theoretical and practical, in the area of engineered systems (e.g. Park et al. 2013; Aven 2011; Dekker et al. 2008; Hollnagel et al. 2006; Sheffi 2007). However, engineered systems as well as production and service processes within these systems are closely related to the human factor, the environment and cybernetic systems. In a globalized society the increasingly interconnected social, technical and economic networks create large complex systems. Thus, there is an urgent need for a comprehensive and holistic approach to the problem of ensuring resilience of such complex systems. This approach requires crossing the boundaries of particular disciplines, and therefore the application of *transdisciplinary perspectives*.

In many research areas the term resilience has been used in a narrow perspective as the ability to return to equilibrium upon a perturbation. In others fields resilience is understood as a capacity to bounce back after disturbance, or recovery to the previous state. From this point of view there is an implicit focus on trying to resist change and control it in order to maintain stability. The approach of *resilience thinking* is even wider, and *deals with complex adaptive system dynamics under deep uncertainty and represents a broad perspective*. Generally resilience thinking has been characterized as the *science of surprise*. In their paper ‘Environmental surprise: expecting the unexpected?’ Kates and Clark (1996) showed that in a complex and intertwined world surprise should be expected. Surprise is understood as a situation when perceived reality departs qualitatively from expectation, and is often shaped by metaphors, and belief systems (Holling 1986). Surprise is not only about shocks and extreme events but also about slower changing and less visible dynamics (Hall and Lamont 2013). Resilience thinking is about the interplay of incremental and abrupt change, of slow and fast variables in complex adaptive systems and how it plays out in uncertain, surprising, and often unpredictable ways (Gunderson and Holling 2002; Carpenter et al. 2009). Resilience thinking is also about deep uncertainty and ‘unknown unknowns’ (Polasky et al. 2011).

Therefore, resilience thinking is about how periods of gradual changes interact with abrupt changes, and refers to the capacity of people, communities, societies, cultures to *adapt or transform* into new development pathways in the face of significant changes, thresholds and tipping points (Folke 2016). Adaptation refers to human actions that sustain development on current pathways, while transformation is connected with shifting development into other emergent pathways and even creating new ones. Therefore, *resilience in its broad sense is a dynamic concept concerned with navigating complexity, uncertainty, and change across levels and scales* (Berkes et al. 2003; Cash et al. 2006; Cumming et al. 2013).

The *adaptability* concept in resilience thinking captures the capacity of people in a social-ecological system to learn using experience and knowledge, innovate, as well as adjust responses to changing external drivers and internal processes. Adaptability has been defined as ‘the capacity of actors in a system to influence resilience’ (Walker et al. 2004) and is about adapting within critical social-ecological thresholds. Adaptability is central to persistence and helps turn changes and surprises into opportunities (Nelson et al. 2007).

Transformability is understood as shifting development into new pathways and creating novelty. It is about having the ability to cross thresholds and move social-ecological systems into new, emergent, and often unknown development trajectories (Walker et al. 2009; Marshall et al. 2012). Disruptions and crises can open up space for transformations, for new ways of thinking and operating, and help in navigating the arising transformative opportunities (Gunderson and Holling 2002; Folke et al. 2009; Chapin et al. 2009). Transformability has been defined as ‘the capacity to create a fundamentally new system when ecological, economic, or social structures make the existing system untenable’ (Walker et al. 2004; Folke et al. 2010).

Resilience, whether for adaptability or transformability, operates and needs to be addressed across levels and scales (Gunderson and Holling 2002). In complex adaptive systems agents interact and connect with each other often in unpredictable and unexpected ways and from such interaction broader scale patterns with new properties emerge (Levin et al. 2013). The resilience of individuals, groups, and communities is tightly coupled to this interplay and the emergent properties of the whole. Because complex adaptive systems have disproportional causation (i.e., small causes can produce big effects) and nonlinearity, they may depict periodic and chaotic dynamics, and potentially irreversible regime shifts (Biggs et al. 2009). Multiple slow and fast drivers of change make it difficult to predict when such changes will occur and to pinpoint cause-and-effect mechanisms (Hughes et al. 2013; Scheffer et al. 2012). Dealing with such complexity and change is facilitated by collaborative and adaptive approaches to management and governance of the biosphere with decision making subject to high degrees of uncertainty and with continuous learning as an important feature (Folke et al. 2005).

The scale, speed, spread, and connectivity of globalization (e.g. global supply networks) create new complex dynamics across levels and domains that play out more and more important role (Walker et al. 2009; Young et al. 2006). Interconnections of systems in a globalized society can propagate and cascade across countries and regions (Adger et al. 2009; Österblom et al. 2015). These interactions and feedbacks are not just global but cross-scale (Lambin and Meyfroid 2011) and their speed may even make the global operate faster than the local. It implies that actions of the local prepare for collaborating with influences from other levels, e.g., political decisions, economic drivers, transnational companies, migration policies, or climate change (Young et al. 2006; Rockstrom et al. 2014). Some of those may be slow creeping influences, others abrupt and unexpected (Scheffer et al. 2012; Homer-Dixon et al. 2015).

The resilience approach would emphasize opportunity of diverse pathways and keeping options to be ready to shift between those within the safe operating space. Resilience research has clarified how phenomena such as flickering, critical slowing down, decreasing recovery rates, and increased variability can serve as ‘early warnings’ of loss of resilience and regime shifts in ecosystems (Hughes et al. 2013; Dakos et al. 2008), and how such signals relate to human behaviour, and the safe-operating spaces of ecosystem regimes (Biggs et al. 2009; Crépin et al. 2012; Schill et al. 2015). The safe-operating space was proposed in relation to zones of

uncertainty with potential thresholds of critical processes at the global level, where regime shifts may challenge essential favourable conditions for human life on Earth (Rockström et al. 2009). There have been attempts to identify surrogates for resilience (Carpenter et al. 2005) as well as sources of resilience (Adger et al. 2005; Goulden et al. 2013) as the idea closely related to the theoretical concept of ‘remember’ for reorganization (Goulden et al. 2013), which has inspired studies on social-ecological memory as critical for resilience building as pockets of social-ecological memory in times of change (Barthel et al. 2010). The role of memory and sources of resilience are addressed in works on deep identities as resilience features in adaptations and transformations (Crane 2010; Tidball et al. 2010; Plieninger and Bieling 2012; Adger et al. 2013; Lyon 2014). Functional diversity and social actor strategies are being increasingly linked in literature (Díaz et al. 2011).

A crucial problem for resilience management in this context is *response diversity*, defined as the diversity of responses to environmental change among species contributing to the same ecosystem function (Elmqvist et al. 2003). Response diversity has been found to be especially important for renewal and reorganization in changing ecosystems (Jansson and Polasky 2010). Resilience assessments are based on a deep understanding of social-ecological system dynamics, recognizing that resilience is a dynamic property influenced by many different processes of interacting fast and slow changing variables, including the larger context and cross-scale (Scholes et al. 2013) as well as unintentional changes of dynamics (Quinlan et al. 2015). The *stewardship* challenge is one of the central problems in resilience thinking (Chapin et al. 2009; Folke et al. 2003) from early work on adaptive management to adaptive governance of social-ecological systems and ecosystem services. Ecosystem services are a key emergent outcome of social-ecological interactions (Reyers et al. 2013). There are some works on management of ecosystem resilience for ecosystem services (Scheffer et al. 2015) with adaptive management as a way of experimenting, learning, and developing understanding for stewardship (Allen et al. 2011).

There are also works on *resilience in relation to legal structures, principles, and processes* (Garmestani et al. 2013), as well as core concepts of the rule of law (Ebbesson 2010) and to the making of normative choices of public interest, public and private responsibilities, and individual rights (Ebbesson and Hey 2013). Cosens (2013) stated that the recognition of the complexity in the social-ecological system requires reform of the administrative state to allow society to responsibly respond to the challenge of managing human interaction with ecosystems.

Resilience approach is increasingly used to manage the *risk of fraud and corruption* in corporate organizations. Bishop and Hydoski (2009) propose a strategy to reduce the vulnerability of organizations to these threats, which consists of three steps: preventing negative events by implementing specific security procedures, detecting and warning about the possibility of such events occurrence, and responding to such events to minimize their adverse effects. This strategy fosters the development of so-called ‘risk intelligence’—that means a conscious, balanced and

dynamic approach to risk management in general and to the risk of fraud and corruption in particular.

In the last decades, the problem of providing resilience to cyber systems and IT has become increasingly important. Cyber-risk has been defined by the Institute for Risk Management (2015) as ‘any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems’. The ISO 27005:2008 defines information security risk as ‘the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization’ (ISO 2008). Typical information security risks include: data leakage, identity and access management failures, data security breaches, system outages, lack of the privacy and application integrity. In order to ensure the robust operation of the systems, especially the complex networks, the most reliable sources of information should be used and the level of the *information quality* should be guaranteed (Linkov et al. 2013). Currently, most attention is devoted to reducing cyber systems vulnerability and, but to a lesser extent, to decrease the consequences of a successful attack, by creating backups of the most important data and information as well as adding new regulations (Gisladdottir et al. 2017).

In the area of *human sciences* resilience is understood as a social-ecological construct, defined as ‘the capacity of individuals to navigate their ways to resources that sustain well-being’ (Ungar 2016). This concept consists of two basic elements (Masten 2015): disturbances (what challenges are threatening the system)—risk factors, and cumulative risk, as well as adversities, chronic or acute, and adaptation (how well the system is doing)—competence in developmental tasks, symptoms and other criteria for judging adaptive success.

Ungar and Liebenberg (2011) proposed the Seven Qualitative Aspects of Resilience:

- A1. Access to material resources (availability of financial, educational, medical and employment assistance, resources, or opportunities, as well as access to food, clothing and shelter).
- A2. Relationships (relations with significant others, peers and adults within one’s family and community).
- A3. Identity (personal and collective senses of purpose, self-appraisal of strengths and weaknesses, aspirations, beliefs and values, including spiritual and religious identification).
- A4. Power and control (experiences of caring for one’s self and others; ability to affect change in one’s social and physical environment in order to access health resources).
- A5. Cultural adherence (adherence to one’s local and global cultural practices, values and beliefs).

- A6. Social justice (experiences related to finding a meaningful role in community and social equality).
- A7. Cohesion (balancing one's personal interests with a sense of responsibility to the greater good; feeling of being a part of something larger than one's self socially and spiritually).

Based on these aspects we can build strategies for positive change (Masten 2015):

- Risk-focused (prevent and reduce risk or adversity exposure).
- Asset-focused (increase resources or access to resources).
- Process-focused (restore or harness the power of human adaptive systems).

Contemporary challenges of the globally intertwined social-ecological systems are serious system challenges, complex, unpredictable, nonlinear, with discontinuous behaviour in space and time and where causes, at times simple, are always multiple (Holling 1986). The cross-scale interactions are effects of centurial accumulation of human influences on air and oceans and transformations of landscapes causing sudden changes in fast environmental variables as well as affecting the health of people, the vitality of societies, and the essential life-support functions of the biosphere (Gunderson et al. 1995). The complex interplay of human actions shaping biosphere capacity has placed humanity in a new situation of interactions of social-ecological systems across scales that are expressed in intertwined, and often turbulent as well as surprising ways (Steffen et al. 2015) affecting people and places in disparate ways.

This situation presents many challenges but also opportunities for adaptation and transformation of social-ecological systems (Westley et al. 2011; Hill and Engle 2013). Resilience management is flexible and open to learning. It attends to slowly changing, fundamental variables that create memory, legacy, diversity, and the capacity to innovate in both social and ecological components of the system. It also conserves, builds experience, and nurtures the diverse elements that are necessary to reorganize and adapt to novel, unexpected, and transformative circumstances (Folke 2016). Specified resilience areas arise in response to the question 'resilience of what to what?' (Carpenter et al. 2001) and for 'whom' (Lebel et al. 2006). But according to the rules of system thinking becoming too focused on specified areas to increase resilience of particular parts or dimensions of a social-ecological system to specific disturbances may cause the system to lose resilience to other disturbances. Specified resilience approaches may be narrowing options for dealing with novel shocks and even increasing the probability of new kinds of instability (Carpenter et al. 2015). It means that sometimes systems becoming very robust to frequent disturbance necessarily become fragile in relation to infrequent ones (Carpenter et al. 2009).

General resilience represents a more broad-spectrum type of resilience for building capacity of systems to adapt or transform in response to the unknown. It applies to all kinds of shocks, including extreme, novel, and unexpected ones (Hall and Lamont 2013). The most important features that characterize general resilience are: diversity, modularity, openness, reserves, feedbacks, nestedness, monitoring,

leadership, and trust (Carpenter et al. 2012). General resilience is also about having the capacity to deal with ongoing gradual change, with deep uncertainty and surprise. Based on empirical work and case studies, Folke et al. (2003) proposed four key features of *general resilience-building* for adaptive capacity, features that interact across temporal and spatial scales and that seem of significance for dealing with dynamics in social-ecological systems:

- F1—learning to live with change and uncertainty;
- F2—nurturing diversity for reorganization and renewal;
- F3—combining different types of knowledge for learning; and
- F4—creating opportunity for self-organization toward social-ecological sustainability.

The F1 emphasizes the significance of accepting uncertainty and surprise, taking advantage of change and crisis, and having the capacity of turning change into opportunity for social-ecological development in tune with the biosphere. The F2 highlights the importance of nurturing diversity for social-ecological resilience, recognizing that diversity is more than insurance against uncertainty and surprise. It also provides the package of components, and their history, that makes development and innovation following disturbance possible. The F3 is about the significance of people's memory, knowledge, experience, and understanding about ecosystem dynamics and their inclusion in management practice and organizations. The F4 brings all these issues together in the context of self-organization, scale, governance, and external drivers, stressing the significance of the dynamic interplay between diversity of the system and disturbances (Folke et al. 2003).

Biggs et al. (2015) have identified a set of seven generic and policy-relevant principles for enhancing resilience of critical ecosystem services for human well-being in the face of disturbance and ongoing change in complex social-ecological systems. These principles are:

- P1—maintain diversity and redundancy (high levels of diversity and redundancy tend to make systems more resilient to change and provide options and flexibility for development),
- P2—manage connectivity (connectivity needs to be managed for sources of resilience, but there is a contradiction between too much connectivity versus modularity in complex systems operating across levels and scales),
- P3—manage slow variables and feedbacks (changes in slow variables and feedbacks should be monitored with supervision systems that can respond in a timely manner, and those supporting biosphere stewardship for ecosystem services should be strengthened),
- P4—foster an understanding of social-ecological systems as complex adaptive systems (with them uncertainty, potential nonlinearities and thresholds),
- P5—encourage learning and experimentation (through experiments and monitoring for enabling adaptive responses),

P6—broaden participation (how it takes place, how is facilitated, and the skills involved, are the key for learning as well as building social capital and collective action),

P7—promote polycentric governance systems (taking an integrative approach that builds on multiple knowledge systems, shifting away from exclusively managing for efficiency toward planning for uncertainty and surprise, creating spaces for spontaneous exploration, and building trust and social capital).

These principles, whether for resilience building, collective action dilemmas (Ostrom 1990), or adaptive governance (Folke et al. 2005), should be approached as processes for generating conditions that allow for resolving collective-action challenges associated with multiple trade-offs in complex social-ecological systems. Such principles support reflection, learning, and adaptation in search of deep understanding of complex, multivariable, nonlinear, cross-scale, and changing social-ecological systems and how to use it for governance of social-ecological systems and ecosystem services (Ostrom 2007; Pahl-Wostl et al. 2012; Biggs et al. 2015; Clarvis et al. 2015).

Increasingly interconnected social, technical and economic networks create large complex systems, and risk assessment of many individual components becomes cost and time prohibitive, or even impossible (Linkov et al. 2014). The uncertainties associated with the vulnerabilities of these systems challenge the ability to understand and manage them. Risk assessment and risk management are no longer sufficient to focus on increasing risks in the modern cyber-physical world having unpredictable situations and scenarios. To address these challenges, risk assessment and management should be used where possible to prepare for and prevent consequences of foreseeable events, but resilience must be built into systems to help them quickly recover and efficiently adapt when adverse events do occur (Linkov et al. 2014).

The National Academy of Sciences identifies four event management cycles that a system needs to maintain to be resilient (NAS 2012):

C1—Plan/Prepare: Lay the foundation to keep services available and assets functioning during a disruptive event.

C2—Absorb: Maintain most critical asset function and service availability while repelling or isolating the disruption.

C3—Recover: Restore all asset function and service availability to their pre-event functionality.

C4—Adapt: Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient.

The Network-Centric Warfare (NCW) doctrine (Alberts 2002) identifies four domains that create shared situational awareness and inform decentralized decision-making; including:

D1—Physical: Physical resources and the capabilities and the design of those resources.

D2—Information: Information and information development about the physical domain.

D3—Cognitive: Use of the information and physical domains to make decisions.

D4—Social nexus: Organization structure and communication for making cognitive decisions.

Linkov et al. (2013) combined the event management cycles and the Network-Centric Warfare (NCW) doctrine to create resilience metrics for cyber systems. Their approach integrates multiple areas of resilience and system response to threats as well as hazards through integrated resilience metrics; however, study of systems as multidomain networks is relatively untypical. Links across specific domains can affect the network's resiliency and should be assessed using network science tools (Abdelzaher and Kott 2013).

Based on the above review of publications related to resilience taken from different areas of knowledge, we will try to create a general concept of complex systems resilience. Thus, in the next part of this section, an attempt will be made to develop an analytical model of resilience, which allows for quantitative evaluation of resilience metrics.

4.2.3 Organisational Resilience—The Concept of Resilient Enterprise

The term 'resilience' is widely used in organizational literature (e.g. Mallak 1998 and 1999; Sutcliffe 2003; Scott et al. 2006; Vogus and Sutcliffe 2007a, b). According to Vogus and Sutcliffe (2007a, b), *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*. Therefore, creating organizational resilience is strongly associated with the people and management concerns (Mallak 1999; Patterson et al. 2007; Vogus and Sutcliffe 2007a, b). By considering the 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 (Boardman and Sausser 2008; Rouse 2005). Gallopín (2006) defines *enterprise resilience* as *an enterprise's adaptive capacity and its ability to cope with, adapt to and recover after a disruption*. He expresses how an enterprise can decrease the level of its vulnerability to expected and unexpected risks, how flexible it is to reorganize itself despite its changing environment, and how effective it may be in recovering in the shortest possible time and at the lowest possible cost. He also states that in order to reduce the susceptibility to potential risks and tolerate the disruptions, 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 the enterprises (Goble et al. 2002).

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. Sheffi and Rice (2005) 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 and have a negative impact on the performance of the system and generate a short- or long-term impact. Sheffi and Rice (2005) define eight phases for disruptive events: A—preparation, B—occurrence of a disruptive event, C—first response, D—initial impact, E—time of full impact, F—preparation for recovery, G—recovery, and H—long term impact (Fig. 4.3). The resilience of the organisation depends on how big a decrease of the system performance was during these phases, and how much time we need from the first impact of the disruptive event to the full recovery. The preparation phase is the time period in which the system can anticipate and prepare for the disruptive event. This phase is very important for increasing a system’s ability to bounce-back from a disruption.

Resilience of an enterprise is measured by the level of its vulnerability to a specific risk (Berkes 2007). *Vulnerability* is defined as being at risk and the likelihood of having disruptions (Christopfer and Peck 2004). Thus, reducing the vulnerabilities has positive impact on the resilience of a system. Reducing

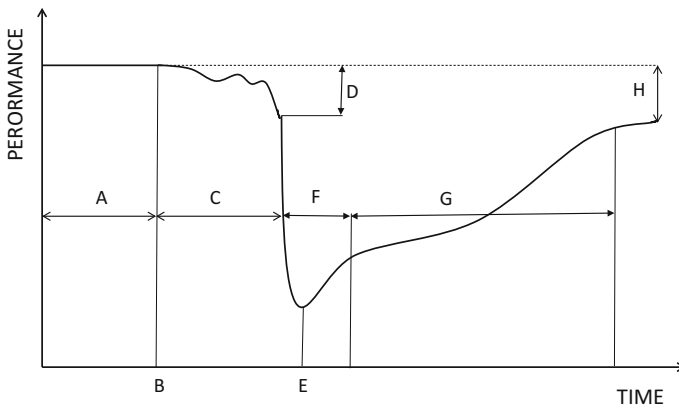


Fig. 4.3 Eight phases for typical disruptive event (based on Sheffi and Rice 2005)

vulnerability means 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 level of its consequences (Sheffi and Rice 2005).

Adaptive capacity is a concept that has been frequently associated with resilience (Dalziell and McManus 2004; Fiksel 2006; Gallopin 2006; Gibbs 2009; Goble et al. 2002; Stevenson and Spring 2007). In order to enhance 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. Dalziell and McManus (2004) identify adaptive capacity as an important metric to evaluate resilience. The adaptive capacity of a system in the case of a disruption can be increased by designing, planning, and building flexibility in organisation (Carpenter et al. 2001; Walker et al. 2004; Sheffi and Rice 2005). *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* (de Leeuw and Volberda 1996; Sushil 2006). Fiksel (2006) describes flexibility as a major system characteristic that contributes to resilience. Hu et al. (2008) states that resilience is a system's ability to bounce back from disruptions and disasters by building in redundancy and flexibility.

The adaptive capacity has been often related to concepts of *robustness*, *agility*, and *adaptability* (Christopfer and Peck 2004; Fricke and Schulz 2005). Robustness characterizes an ability to be insensitive towards changing environments, and agility indicates an ability to change rapidly, whereas adaptability shows an ability to adapt towards changing environments while delivering 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 (Carpenter et al. 2001; Christopfer and Peck 2009; Walker et al. 2002). Helaakoski et al. (2007) defines agility as a system's ability to respond quickly to changes in an uncertain and changing environment. According to Christopher and Peck (2004), resilience involves agility and it helps an organisation itself to reorganize rapidly against the changing environment, while Morello (2001) suggests that agility may introduce new risks and vulnerabilities which result in lower resilience.

Information and *connectivity* are next essential elements of resilience (Horne 1997). Creating enterprise resilience relies on perceiving environmental change quickly and implementing adaptive responses early (Weick and Sutcliffe 2001). Effective use of enterprise information systems can improve decision-making abilities of the organisation that result in increased flexibility, agility, and adaptability, all of which are supporting attributes of resilience (Fiksel 2006; Haimes et al. 2008; Helaakoski et al. 2007).

Erol et al. (2010) suggests two key enablers of enterprise resilience. First of them is the capability of an enterprise to connect people, processes, and information in a way that allows this organisation to become more flexible and responsive to the dynamics of its environment, stakeholders, and competitors. Such connectivity requires integration within the enterprise and across the partners, suppliers, and

customers of the enterprise. The second enabler is coordination of information technology and business goals. Attaining this requires simplification of the underlying technology infrastructure and creation of a consolidated view of, and access to, all available resources in the enterprise. Enterprise architecture provides a simple and consolidated view of the enterprise and supports the integration and connectivity at inter and intra enterprise levels (Erol et al. 2010).

Enterprise integration connects and combines subsystems to ensure the adequate people, processes, information and physical resources all come together at the right times. Enterprise integration helps to establish a technology infrastructure that links its complex enterprise subsystems into a homogenous system of systems, in which the processes and the data can be shared across the company, with business partners, and with customers (Brosey et al. 2001; Kosanke et al. 1999; Smith et al. 2002; Venkatachalam 2006). Data integration is the basic level of enterprise integration and requires semantic compatibility as well as exchange of information on this level (Huang et al. 2003). As a result of data integration, different kind of applications can exchange information and compatibility can be achieved between business processes and infrastructure systems (Venkatachalam 2006). Process integration is understood as combining into one coherent whole of business processes across multiple systems and environments within or across enterprises (Themistocleous and Corbitt 2006; Zhu et al. 2004). Process integration increases the efficiency of the enterprise and its ability to compete in terms of its cost, service capabilities, and responsiveness (Lam 2005; Stohr and Nickerson 2003). Enterprise systems integration focuses on information and data integration at application level (Hasselbring 2000; Raut and Basavaraja 2003; Themistocleous and Corbitt 2006). The primary purpose of enterprise systems integration is to access and share data about the business processes (Cummins 2002; Irani et al. 2003; Yang and Lu 2005).

Enterprise architecture is an important instrument in addressing the alignment of business and technology as well as achieving enterprise integration (Goethal et al. 2004; Kühnle and Wagenhaus 2005). Enterprise architecture provides a common view of both the primary resources of any enterprise (people, processes and technology), and how they integrate to support the primary drivers of the enterprise (Anaya 2005). According to ANSI/IEEE Standard 1471–2000, architecture is defined as the ‘fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution’ (IEEE 2000). Zachman (1987) describes enterprise architecture as a set of descriptive representations that are relevant for modelling an enterprise management’s requirements over the period of its useful life. A properly designed enterprise architecture supports enterprise integration by enabling the common view of business processes, data, and systems across the enterprise and its partners (Bernus et al. 2003; Kosanke and Nell 1997; Petrie 1992; Vernadat 1996). It is also an important tool to create connectivity within the extended enterprise and help achieve agility and flexibility (Goethal et al. 2004; Helaakoski et al. 2007).

Enterprise resilience also requires interoperability and integration between the processes, systems, and underlying technology across business partners. Service oriented architecture (SOA) is a widely accepted approach in enterprise information

systems development and enterprise integration (Erl 2007). SOA simplifies the development of enterprise applications as modular, reusable business services that are easily integrated, changed and maintained. By adopting an SOA approach and implementing it with the use of supporting technologies, companies can build flexible systems that realise changing business processes quickly, and make extensive use of reusable components (IBM 2005). SOA supports an information environment built upon loosely coupled, reusable, standards-based services.

Summarising we can define enterprise resilience as a function of robustness, flexibility, agility, adaptability, and finally efficiency. 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.

4.2.4 From Resilient Enterprise Concept to Process Continuity Ensuring

Organizations often face variable and unpredictable situations which threaten their profitability and existence. All business is exposed to risks from their surroundings in many different scenarios, e.g. regional power outages, natural disasters, acts of terror or economic downturns which can seriously damage enterprise operations. The result of these threats can be a business disruption (loss of business continuity), or other important consequences such as: market share loss, productivity fall, regulatory noncompliance and reputation damage.

Business continuity can be defined as an effort within organizations, aimed to ensure that critical functions keep their operational status, during a wide range of emergencies, including localized acts of nature, accidents, technological or attack-related emergencies. Business continuity management is an actual approach to keep on business service and operations during the occurrence of a disruptive event, IT related, business related, or a natural disaster (Giaccherro et al. 2013). Its main goals are:

- quickly responding to any threat;
- capturing all opportunities;
- avoiding disruptive events;
- preventing security attacks;
- lessening impact of other catastrophic events.

Usually accidents occur from a combination of active failures and latent conditions (Reason 2008). The resulting damage can be so serious that one or more infrastructure components can be unavailable for a long time, because disruptive events still affect operations long after the event itself was solved. When disasters occur, the very short run determines whether—and how—an organization will go

past it. In order to achieve a long-term business survival after a disaster, a short-term continuity of operations is essential (Stead and Smallman 1999).

Business continuity management supports preventing, responding to, managing and recovering from fallouts of an incident or a disruptive event. It assists in maintaining uninterrupted availability of all resources required for essential business operations. Business continuity planning is therefore that part of operational risk management that establishes the correct reactions and the best cost-effective measures to be taken when a disruptive event occurs, in order to avoid business interruptions (Giaccherro et al. 2013).

Government and regulatory agencies develop requirements and legislative measures to face critical events. The British Standards Institution published the ‘Guide to Business Continuity Management’, which recommends a holistic approach to draw up a program to increase organisation operational resilience level (BSI 2003). The US National Fire Protection Association provided the Standard NFPA 1600, the foundation for disaster/emergency management planning and business continuity programs, both in private and public sectors, suggesting common program elements, techniques, and processes (NFPA 2013).

Business continuity strategy creates a culture within the organization, which aims to increase resilience level as well as to ensure stability in products and service delivery. These practices should be carried even on ‘normal’ accidents, due to the increasing complexity and tight bound between people and technology (Perrow 1994; Cacciabue 2004). Managing business continuity, we should not use the likelihood of accidents as the main criterion in approaching risks, but rather business impact of this events instead. Potential *adverse event* types can be classified as follows (Vancoppenolle 2007):

- failure of an isolated infrastructure element (e.g. single points of failure);
- long-term interruption of a critical information flow;
- long-term interruption of a critical business process;
- local long-term business interruption;
- complete business interruption.

The business continuity management should therefore address the effect of those events on operations (e.g. infrastructure, IT, networks, etc.) and solve the issues caused by the events themselves, in order to keep business running. A business continuity management program should be integrated into the company culture and be owned by everyone within an organization (Giaccherro et al. 2013).

While a simple business continuity planning concerns protection of business operations and processes, a *resilient strategy* extends the boundaries of protection beyond unexpected events and disasters to include any changes from normal business activities, resulting from adverse events. A resilience program exploits opportunities to minimize operational, financial, legal and reputational risks that arise from a disruption. The goal is to empower enterprises with the capability to promptly adjust and transform business in response to any change in order to manage threats and opportunities, create competitive position and improve

shareholder value. A resilience program contributes to develop effective long-term strategies, ensuring actions properly aligned to enterprise's risk appetite and aversion (Giaccherro et al. 2013). Resilience is a property intimately related to the organizations ability to avoid, contain and mitigate accidents (Manyena 2006), and has three main dimensions (Westrum 2006):

- the capability to prevent an accident from occurring;
- the capability to avoid that an occurred accident propagates (e.g. cascading failures);
- the capability to recover to the normal state, after an occurred accident.

A resilience strategy plan helps reducing the actual impact of disruptive events to business, through the identification of potential weaknesses, and precise definition of what is to be looked for (e.g. performance monitoring) and what to expect (e.g. how to anticipate threats in the future) (Hollnagel 2009). Thus, first it is necessary to establish what exactly the requirements are, to survive despite unexpected events and then to plan how to overcome challenges that could come at any time. The ability in disaster recovering can also be improved by both pre-event and post-event activities (McDaniels et al. 2008), in order to mitigate and be prepared to the initial impact of a disaster. The concept of resilience can be used for strategic decision-making, if it offers a means to consider the relative risk of each alternative scenarios. Thus, the enterprise success relies upon its ability to be resilient, which allows it to take full advantage of changes in its business environment and to anticipate unexpected events and risks. This approach to resilience can proactively help facing adverse events, in order to minimize damages and to maximize return on investment from assets.

If a major incident occurs, the organization should be able to *maintain the continuity of its operations* and protect the stakeholders' interests. Certainly, the main goal of a business resilience program is to protect critical operations, services and resources and to maintain business continuity. An organization should carry out this goal according to its strategy, which should be systematic and proactive in order to anticipate future business changes and discontinuities. A strong resilience strategy should reduce waste of time and money, since it is a so called 'ready-right-from-the-start' strategy, not just a routine to recover from unwanted event.

An effective business resilience program, requiring strong efforts in business continuity and disaster recovery activities in order to ensure the proper resilience level for critical operations, should also have a focus on ICT infrastructure. It requires focusing on advanced security technologies, and organizations rely deeply on automation and on those elements of the physical infrastructure that support automation, such as telecommunications, information systems, and electrical systems availability. Protecting a company with investment in information systems is costly but indispensable to survive and stay competitive; thus, the growing reliance on information systems increases the risk of ICT system outage. Managing and mitigating risk requires an agile network architecture that can guarantee low latency

and high availability for real-time applications, maintaining security in access control at the same time. It is very important to ensure reliable and timely delivery of critical applications and data and to respond—with flexibility—to changing business requirements (Giaccherro et al. 2013).

The Basel Committee on Banking Supervision defined *business resilience* as ‘the skill to absorb the impact of a major disruption while maintaining operational each critical activity or service’. It also classified the IT risk as an operational risk, defined as ‘the risk of loss resulting from business disruption and system failures, related to hardware, software, telecommunications and utility outage/disruptions’ (Basel Committee on Banking Supervision 2006a, b). That means there exists a strong correlation between IT and operational risks. Banks and many other organizations, have increasingly linked their business performance to information systems. The result is that IT has taken a very important and critical role in the operational processes continuity, becoming one of the major sources of operational risk.

IT risk is linked with many aspects of business operations: business environment, quality control processes and information flows. Organizations rely entirely on IT infrastructures to protect business from a wide range of security threats, more than just technology failures or disruptions. From the IT perspective, risk management has to (Giaccherro et al. 2013):

- assess and determine potential losses due to accidents or disasters in electrical infrastructure;
- implement plans and strategies to deal with the issue of contingency planning, deciding whether a contingency plan or business continuity plan is appropriate for the enterprises;
- develop hardware and software strategies to achieve the best recovery arrangement for IT systems;
- provide off-site storage facilities to ensure that critical data are properly protected.

Unexpected events occur quite often because of intrinsic organization weaknesses, e.g. vulnerable IT systems, lack of operator training, process variations, incorrectly followed routines, and many other.

The ANSI 942 standard (ANSI 2008) classifies four different levels of system architectures, or ‘tiers’, each one with specific performance levels. This approach is based on the system engineering vision, therefore being compliant with the holistic view prescribed for operational risk management. The standard describes the prescription that a system has to reach each tier specification:

- Tier 1 (basic architecture). It is only capable to supply its users, without redundancy within or between its subsystems. Every planned maintenance operation must be completed during power off period, and every system failure will cause an operational disruption. Perceived availability statistically results to be 99.67%, correspondent to 28 h per year of downtime for a system working in a continuous mode (so called 24/7 system).

- Tier 2 (redundant capacity components architecture). Its configurations require at least $N + 1$ redundant active components, with a single distribution path. Tier 2 topology does not allow scheduled online maintenance. Moreover, in this configuration some kind of active components failure may however disrupt business continuity. Perceived availability is 99.75%, correspondent to 22 h per year of downtime.
- Tier 3 (concurrently maintainable architecture). Its architectures, in addition to tier 2 specification, require at least a $N + 1$ redundant configuration for each subsystem. Moreover, two different distribution paths and two different power sources should be designed, with only one active at a time. Thus, it is possible to disconnect each component without influencing operational continuity. In order to obtain a concurrently maintainability standard, every user should be connected properly to both distribution lines. Perceived availability is 99.98%, correspondent to 4 h of down time every 2.5 years, and it is not necessary to disconnect the IT load during the scheduled maintenance.
- Tier 4 (fault tolerant architecture). This type of architecture is designed to have a completely redundant configuration, which ensures that every failure of each component will not be critical for the IT load. Each path must be compartmentalized, therefore a single failure event cannot affect the distribution subsystem. Using this architecture, the operational continuity is granted against each failure and most of voluntary unwanted operations (maintenance errors, sabotages, etc.). Perceived availability is 99.99%, correspondent to less than 4 h failure every 2.5 years.

This classification can help in optimizing the total costs of a business continuity plan. If scheduled maintenance downtimes are allowed, according to the plan, a Tier 2 design can be the proper design choice. However, if the criticality requires a full ‘24/7 operational service’, usually the highest performance level, thus the Tier 4 system will be needed. This leads to get so called ‘five nine’ availability level (i.e. 99.999%) for the IT system, which is almost unreachable, because in practice it means less than a single failure within 45 years. Thus, the realistic goal of an organisation is to maximize the availability rate, starting from its infrastructure reliability.

Summarizing an effective business continuity programme will provide widespread benefits for any organisation by (based on Deloitte 2018):

- improving awareness about threats and vulnerabilities;
- protecting people, reputation and shareholder value;
- increasing supply chains resilience;
- determining and protecting time-critical business processes;
- meeting customer and regulatory demands;
- accelerating effective decision-making in any crisis situation;
- improving the ability to respond to major incidents effectively and efficiently;
- providing more favourable conditions when negotiating business interruption insurance premiums.

4.3 Managing Operational Risk—The Concept of Dependable Operating

4.3.1 From Reliability Engineering to Dependability Engineering

Reliability Engineering as a scientific discipline was born in the mid-1950s, and has been developing particularly rapidly since it was integrated into risk assessment methodology in 1970s (Saleh and Marais 2006). With the increasing complexity of systems having a multidimensional character, as well as growing levels of uncertainty and risk, classic methods of assessing reliability have become insufficient. An in-depth analysis of the unsolved problems and new challenges facing reliability engineering was presented by Zio in 2009 and seems to be still valid (Zio 2009).

In the areas of technical sciences, particularly fast-growing ones (such as computer science), at the end of the 20th century there began to form concepts of a comprehensive approach to the issues covered by reliability engineering and extended additionally by problems related to safety and security of systems (e.g. Anderson 2008; Leveson 2008; Stephans 2004). There has been proposed a concept of dependability, as a collective term to describe the availability of a system, and its influencing factors, namely: reliability, maintainability and maintenance support performance (Avizienis et al. 2004). Over time, new concepts of the term ‘dependability’ were created, focused on the specific nature of the field in which they could be applicable. As a result of these works there began to emerge in the IT area, on the basis of reliability engineering, its generalized version—dependability engineering (Kaâniche et al. 2000; IEC 2015). A significant advantage of this concept, especially for systems with high complexity, is its service orientation and risk related approach, but disadvantage can be represented by its close fit to the computer area specificity.

Another problem was related to the difficulty of defining the relationship between the concept of dependability and other similar concepts, such as: survivability and trustworthiness (Avizienis et al. 2004) as well as resilience (e.g. Hollnagel et al. 2006). The reason for such a large interest in this area appears to be primarily due to the growing importance of the threats and hazards of the type ‘LSLIRE’ (large scale, large impact, rare events) (Aven 2015; Taleb 2007, 2012). Events of this type are particularly dangerous for system of systems such as critical infrastructure (e.g. El-Thalji 2011; Kröger and Zio 2011; Shafieezadeh and Burden 2014; Zio 2007) and global supply chains (e.g. Bosman 2006; Kleindorfer and Saad 2005; Natarajarathinam et al. 2009; Sheffi and Rice 2005; Straube and Pfohl 2009; Waters 2007).

Thus, it is fully justified to seek opportunities to generalize the concept of dependability in a way, that could be applied to all types of complex systems operating under both normal and abnormal work conditions. The first step towards solving this problem is to overview the basic concepts, principles and models existing in this field and subsequently, there should be developed the overall

concept of dependability, applicable to all complex engineered systems, such as large scale and ultra large scale systems, in particular.

(a) *Availability related concept of dependability—a probabilistic approach*

IEC Technical Committee 56 was formed in 1965 as “Reliability and Maintainability” to prepare international standards that cover generic aspects of Reliability Engineering in the electro-technical field. In 1989 the initial title of IEC TC 56 was changed to ‘Dependability’, and in 1990 after consultations with ISO (especially quality related ISO 9000) the scope of the Committee was extended to the generic dependability issues across all technological disciplines. Based on these standards IEC 60050-191 and IEC 60300-1 (IEC 2015) dependability reflects user’s confidence in fitness for use by attaining with satisfaction in product performance capability, delivering service availability upon demand, and minimizing the costs associated with the acquisition and the ownership throughout the life cycle. In this context, the product is understood as a simple item (for example a material, a device, an algorithm) or a complex system (for example transportation system or an integrated network comprising of hardware, software and human elements).

Dependability is defined as the collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance and it should be applied only for general, non-quantitative descriptions. Availability performance is the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided. An item is defined as any part, component, device, subsystem, functional unit, equipment or system that can be individually considered.

The influencing factors of availability are defined as following:

- Reliability performance is the ability of an item to perform a required function under given conditions for a given time interval.
- Maintainability performance is the ability of an item under given conditions of use, to be retained in, or restored to a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources.
- Maintenance support performance is the ability of a maintenance organization, under given conditions, to provide upon demand, the resources required to maintain an item, under a given maintenance policy.

A method of practical use of this concept has been presented in the standard IEC 60300-3-4 (Dependability management—Part 3: Application guide—Section 4: Guide to the specification of dependability requirements) (IEC 2015). In the Annex A of this guide some examples of reliability, maintainability, maintenance support and availability requirements are presented. As reliability performance measures are proposed: mean failure rate— $\lambda_m(t_1, t_2)$, mean time to failure—MTTF,

mean failure intensity— $z_m(t_1, t_2)$, mean time between failures—MTBF, useful life— T_u and reliability function— $R(t_1, t_2)$. The most commonly used indicators for maintainability are: mean repair time—MRT and mean time to restoration—MTTR. The typical measures for maintenance support are: mean administrative delay—MAD and mean logistic delay—MLD. As availability requirements are specified: mean availability— $A_m(t_1, t_2)$, mean unavailability— $U_m(t_1, t_2)$ and mean down time—MDT. So the specification of dependability requirements for a time period (t_1, t_2) could be represented by the exemplary vector:

$$D = \{A(t_1, t_2); \lambda_m(t_1, t_2); R(t_1, t_2); MTBF; MTTF; MTTR; MRT; MAD; MLD; MDT\} \quad (4.1)$$

where the D-vector components are parameters of random variables distributions.

Estimating these parameters with statistical methods requires an adequate sample size, which is not always possible. This is particularly the case for systems characterized by high level of reliability and of particularly rare threats and hazards.

(b) *Availability and credibility related concept of dependability—a probabilistic-deterministic approach*

The starting point for this consideration was the concept of dependability presented in the standard IEC 61069 “Industrial-process measurement and control—Evaluation of system properties for the purpose of system assessment”, Part 5 “Assessment of system dependability”. In this standard the term *dependability* is defined as: *the extent to which a system can be relied upon to perform exclusively and correctly a task under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided. Dependability has two components of its property: availability as probabilistic component and credibility as deterministic ones.* The definition of availability is exactly the same as in the IEC 60300-1 (IEC 2015), and its performance measures can be created in the same way, that is with support of statistical tools. *Credibility* is defined as the extent to which a system is able to recognize and signal the state of the system and to withstand incorrect inputs or unauthorized access. This deterministic property consists of the two components: integrity and security. Integrity is understood as the assurance provided by a system that the task will be performed correctly unless notice is given any state of the system, which could lead to the contrary. Security is the assurance provided by a system that any incorrect input, or unauthorized access is denied.

This concept was used by Bukowski and Feliks (2005, 2008), as the basis for the design of an expert model to assess the system dependability. In these works the term credibility (CR) was understood as an amalgam of safety (SAF) and security (SEC). There was proposed the following model for credibility measure:

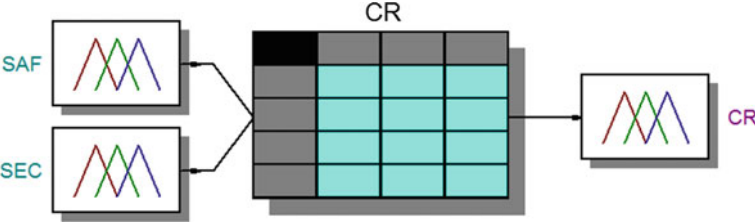


Fig. 4.4 The structure of the credibility evaluation fuzzy system (Bukowski and Feliks 2008)

$$CR = \{SAF \cap SEC\}$$

(4.2)

and to use fuzzy logic procedure as well as linguistic variables to describe the expert knowledge about safety and security. The general structure of the credibility evaluation system is shown in Fig. 4.4.

A base of rules for a system with two inputs and one output, where every variable was divided into 5 linguistic categories (Very Low, Low, Moderate, High and Very High), includes 25 elements. The correctness of selection of rules as well as the shape and ranges of the membership function is verified with a rules viewer and simulation procedures. The rules viewer displays a roadmap of the whole fuzzy inference process. It also shows how the shape of certain membership functions influences the overall result. Figure 4.5 presents a simulation model of a credibility evaluation system and the results of a simulation in the form of a graph showing the dependence of the output variable on the input variables.

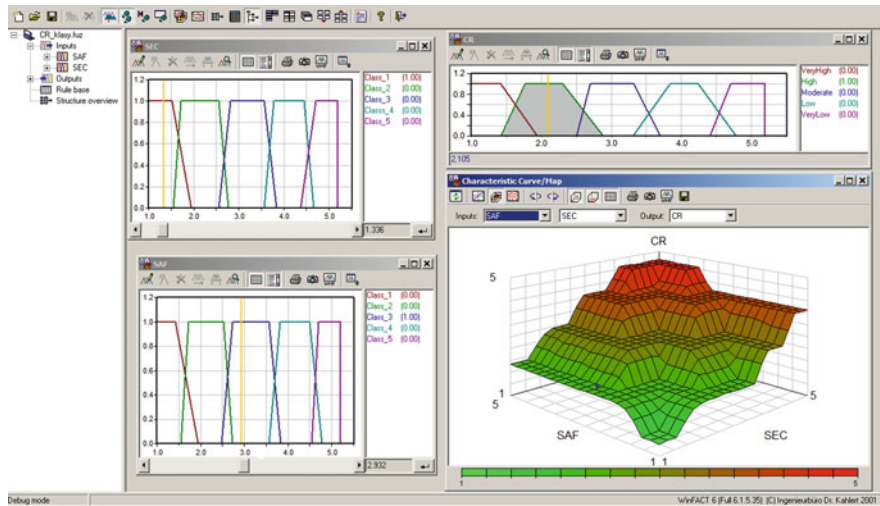


Fig. 4.5 Credibility simulation model and its results (Bukowski and Feliks 2008)

This model of the deterministic part (credibility) can be integrated with the classical probabilistic part (availability) using fuzzification procedures.

(c) *The concept of dependable service delivery—a risk related approach*

In 1956 J. von Neumann, E. F. Moore and C. E. Shannon developed theories of using redundancy to build reliable logic structures from less reliable components, whose faults were masked by the presence of multiple redundant components. The theories of masking redundancy were unified by Pierce (1965) as the concept of *failure tolerance*. In 1967, A. Avizienis integrated masking with the practical techniques of error detection, fault diagnosis, and recovery into the concept of *fault-tolerant systems*, and 8 years later work on software fault tolerance was done by B. Randell. The emergence of a consistent set of new concepts and terminology resulted in the book “Dependability: Basic Concepts and Terminology” by J.-C. Laprie in 1992 and a new research area *Dependable Computing* was born.

The contribution brought by the computer system group is represented in the dependability tree. The authors developed the concept of fault-tolerant computing, based on the idea of *dependable service delivery* proposed in the work “Basic concepts and taxonomy of dependable and secure computing” (Avizienis et al. 2004). In the work the dependability of a system is understood as *the ability to deliver service that can justifiably be trusted*. This definition stresses the need for justification of trust. The criterion for justification of system dependability is based on the concept of risk, and is defined as follows: *dependability of a system is the ability to avoid service failures that are more frequent and more severe than it is acceptable*.

The service delivered by a system is manifested in its behaviour as it is perceived by its user(s); a user is another system (physical or human) that interacts with the former at the service interface. The function of a system is what the system is intended for, and is described by the system specification. Dependability is an integrative concept that consists of three parts: the attributes of, the means by, and the threats to which dependability is attained.

Dependability attributes:

- availability—readiness for correct service;
- reliability—continuity of correct service;
- safety—absence of catastrophic consequences on the users and the environment;
- confidentiality—absence of unauthorized disclosure of information;
- integrity—absence of improper system state alterations;
- maintainability—ability to undergo repairs and modifications.

Dependability means:

- fault prevention—how to prevent the occurrence or introduction of faults;
- fault tolerance—how to deliver correct service in the presence of faults (e.g. redundancy);

- fault removal—how to reduce the number or severity of faults (e.g. corrective or preventive maintenance);
- fault forecasting—how to estimate the present number, the future incidence, and the likely consequences of faults.

Dependability threats:

- faults,
- errors,
- failures.

Security is the concurrent existence of:

- availability for authorized users only,
- confidentiality,
- integrity with ‘improper’ meaning ‘unauthorized’.

Correct service is delivered when the service implements the system function. A *failure* is an event that occurs when the delivered service deviates from a correct service. A system may fail either because it does not comply with the specification, or because the specification did not adequately describe its function. A failure is a transition from correct service to incorrect service, i.e., to not implementing the system function. A transition from incorrect service to correct service is a *service restoration*. The time interval during which incorrect service is delivered is a *service outage*. An *error* is that part of the system state that may cause a subsequent failure: a failure occurs when an error reaches the service interface and alters the service. A *fault* is the adjudged or hypothesized cause of an error. A fault is active when it produces an error, otherwise it is dormant. A system can fail in the different ways—failure modes.

The *concept of fault-tolerant computing* became very successful in the area of information technology and computer science, but was not general enough, to cover all types of engineered systems, e.g. global production systems and logistics networks, especially in presence of the low frequent and unpredictable hazards.

4.3.2 Disruption-Tolerant Operating—The Continuity Oriented Approach

(a) The concept of disruption tolerant networking

The Delay- and Disruption-Tolerant Network (DTN) is a network of smaller networks. It is an overlay on top of special-purpose networks, including the Internet. DTN supports interoperability of other networks by accommodating long disruptions and delays between and within those networks, and by translating different communication protocols of those networks (DTN 2012). The concept of DTN was originally developed for interplanetary use, where the delay-tolerance is the extreme need. However, DTNs may have diverse applications on Earth, where disruption-tolerance

is the highest need. The potential Earth applications span a broad range of commercial, scientific, military, and public-service applications (DTN 2012).

DTNs can use many kinds of wireless solutions, including radio frequency (RF), ultra-wide band (UWB), free-space optical, and acoustic (sonar or ultrasonic) technologies.

Many evolving and potential communication environments are characterized by:

- Intermittent connectivity—the absence of an end-to-end path between source and destination (so-called network partitioning).
- Long or variable delay—long propagation delays between nodes and variable queuing time at nodes contribute to end-to-end path delays.
- Asymmetric data rates—the Internet supports moderate asymmetries of bidirectional data rate, but if asymmetries are large, they defeat conversational protocols.
- High error rates—bit errors on links require correction or retransmission of the entire packet.

DTN overcomes the problems associated with intermittent connectivity, long or variable delay, asymmetric data rates, and high error rates by using *store-and-forward message switching*. This is an old method, used by postal systems since ancient times. Whole messages (e.g. entire blocks of user data) or fragments (parts) of such messages are moved forward from a storage place on one node (so-called switch intersection) to a storage place on another node, along a path to the given destination. The storage places (e.g. hard disks) can hold messages indefinitely, and they are called *persistent storage*, as opposed to very short-term storage provided by memory chips and buffers.

DTN routers need persistent storage for one of the following reasons:

- A communication link to the next ‘hop’ may not be available for a long time.
- One node in a communicating pair may send or receive data much faster or more reliably than the other node.
- A once transmitted message may need to be retransmitted if an error occurs at an upstream (toward the destination) node, or if an upstream node declines acceptance of a forwarded message.

DTN supports communication between intermittently connected nodes by isolating delay and disruptions with a store-and-forward technique. The intermittent connectivity may be opportunistic or scheduled (DTN 2012).

The DTN store-and-forward message switching architecture is a generalization of work originally conceived to support the InterPlaNetary Internet (IPN). The primary goals are interoperability across network environments, and reliability capable of surviving hardware (network) and software (protocol) failures. DTNs also may have many logistics applications, namely:

- cargo and vehicle tracking (by road, rail, sea, and air),
- autonomous vehicles communication and control,
- smart transportation networks,
- in-store and in-warehouse asset tracking,
- data transactions,

- processing-plant monitoring,
- infrastructure-integrity monitoring,
- disaster communication,
- atmospheric and oceanographic conditions,
- seismological events.

(b) *The continuity oriented approach*

The continuity oriented approach is closely related to the idea of resilient enterprise (Sheffi 2007) as well as the concept of disruption-tolerant operation (Bukowski 2016). From the operational perspective, the typical ‘mess’ (see Sect. 3.1.1) for complex engineered systems is caused by losing the continuity of production or service processes. This type of risk sources is called disturbance and can lead to disruptive event in a given system. The behavior of the system in ‘mess’ situations depends to a large extent on system’s structure and its operational features. Table 4.3 shows the summary of the basic operational features for the main types of systems. The basic issue for our consideration is the problem of how the system behaves in response to disturbances. We can distinguish four basic types of responses: resistance, robustness, absorption and recovery, as well as learning and adaptation.

The model proposed below is based on a typical course of a system operating process, interrupted by an occurrence of a disruptive event leading to a disruption of this process continuity. An example of such a course as a function of time is represented in Fig. 4.6 (based on Bukowski 2016), in which there can be distinguished four fundamental phases:

- I. *Reliable state*. Resistant (no reaction to small disturbances) and robust behaviour (short-term loss of performance after a disturbance and rapid return to the required state). A phase of normal operation (*full availability* of system), interrupted only by slight disturbances and rare cases of more serious threats or hazards, recognized sufficiently early and ‘parried’ (thwarted), thanks to a properly functioning: supervision (e.g. anticipation and recognition of risk sources), prevention and protection subsystems.
- II. *Absorption behavior*. Coping with disruption and retaining the continuity of operation. A phase of process continuity disruption, happening directly after an occurrence of a threat, which has not been effectively blocked by the

Table 4.3 The main types of systems and their operational features

Type	Complexity	State adjustment	Response to disturbances	Example
I—Passive	Low	Constant	Resistance	Elements
II—Reactive	Medium	Static control	Robustness	Parts
III—Responsive	High	Dynamic control	Absorption & recovery	Subsystems
IV—Active	Very high	Smart control	Learning & adaptation	System of systems

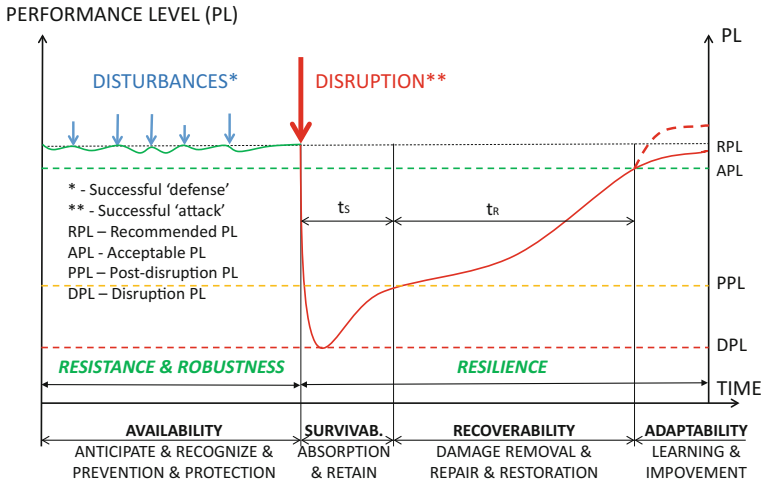


Fig. 4.6 A typical course of an operating process with a failure occurrence

- protection subsystem. During this phase, the system's *survivability* is its essential property, which is measured by the disruption performance level (DPL) and the post-disruption performance level (PPL), as well as the time t_s .
- III. *Recovery*. A phase of damage removal, system's repair and restoration to an acceptable performance level (APL) after the process continuity disruption, characterized by the APL and the time t_r (*recoverability* through bounce back to acceptable performance level).
 - IV. *Adaptation*. Performance improvement phase through learning from disruption and transformation to the new work conditions (adaptability thanks flexibility and agility).

In phase I, under normal work conditions, the availability and security perspective dominate, while in the phases II and III, under abnormal work conditions, it is resilience and safety perspective that have the decisive influence on the operating quality of a given system. After the removal of the negative effects of the process continuity disruption, a process of the improvement can begin, consisting in an adaptation of the system to new working conditions and a possible increase in the level of performance (phase IV). However, if the renewal process would not be successful, it will be necessary reengineering of the system (e.g. a new design of structure and processes).

4.3.3 Operational Risk Based Concept of Dependability

On the basis of the considerations set out above (in Sects. 4.3.1 and 4.3.2) there will be proposed a generalized model of dependability, intended for the application

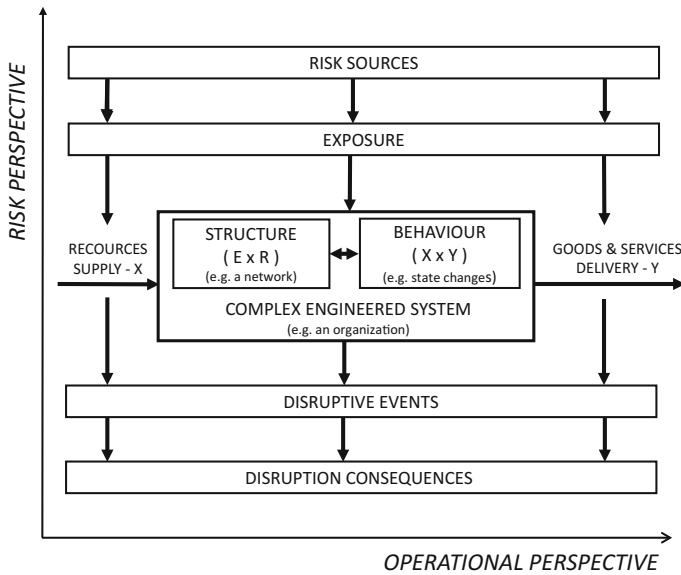


Fig. 4.7 General model of a complex engineered system in two-dimensional perspective

within complex engineered systems. According to the assumptions from Sect. 3.3.2, we understand *the dependability as a collective term describing the time-related operating quality of a system*.

Figure 4.7 shows a general model of a complex engineered system with a defined structure $\langle E \times R \rangle$ and behavior $\langle X \times Y \rangle$ in the two-dimensional perspective. From an operational perspective the system inputs X are controllable events (supply of resources), and its outputs Y are the produced functions (delivery of goods and services). In the risk perspective however, the system inputs are the uncontrollable events occurring in its environment (disturbances), and its outputs stand for possible disruptive events. This model can provide a basis for analyzing the dependability of a complex engineered system which operates in a risky environment, using *the continuity oriented approach*.

We propose to base the quantitative dependability assessment on the concept of risk (Sect. 2.3), as well as vulnerability and resilience (defined in Sect. 3.3.2). The concept of vulnerability is founded on three main elements (Kröger and Zio 2011):

- Degree of loss and damages due to the impact of disruptive events;
- Degree of exposure to the risk sources, i.e., likelihood of being exposed to threats and hazards of a certain degree and susceptibility of an element at the risk of suffering loss and damages;
- Degree of resilience, i.e., the ability of a system to anticipate, cope with/absorb, resist and recover from the impact of a threat (technical) or hazard (social).

In general, we understand *vulnerability to a disruptive event* as the degree to which a system is affected by a disruptive event and the term *dependability* as ‘anti-vulnerability’.

The evaluation of the dependability for complex engineered systems is a process that can be represented in the form of the general algorithm presented in Fig. 4.8. The method is implemented in 10 stages. At the beginning, the system under investigation should be precisely defined. Then, a team of experts select potential sources of risk $\{RS_i\}$ based on the literature, data and their own experience. The set of identified risk sources is the basis for generating potential risky scenarios $\{TH_j\}$, which actually (although sometimes with a very low probability) may occur within the analysed system. A team of experts assess the occurring likelihood for each of these scenarios $P(TH_j)$.

A properly designed complex engineered system should be equipped with a security system consisting of a number of proactive barriers $\{PB_k\}$, which in turn are designed to prevent direct exposure of the system to a loss of its ability to perform the function. Thus, the next step is to assess the efficacy of these barriers $\{E(PB_k)\}$ for each of the potentially possible risky scenarios $\{TH_i\}$. These risks, which are not effectively blocked by security barriers, become direct system exposures $\{EX_i\}$ and are defined as the initiating events that can interrupt the continuity of a process $\{DE_m\}$ (disruptive events). For these events there are

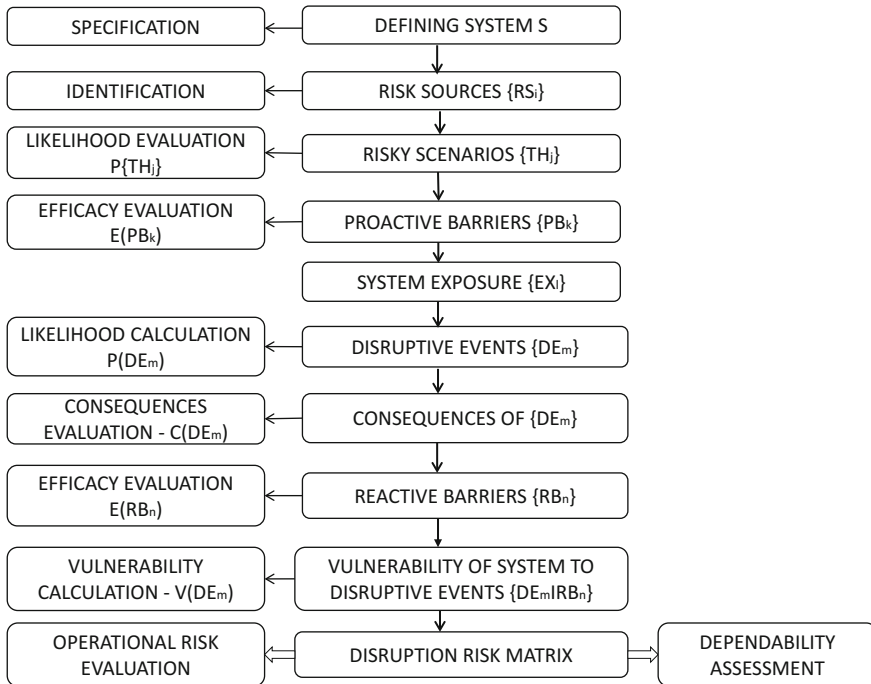


Fig. 4.8 The evaluation algorithm of the dependability for complex engineered systems

calculated the measures of uncertainty of their occurrence, e.g. in the form of probabilities $\{P(DE_m)\}$, as the product of the likelihood for each of scenarios $\{P(TH_j)\}$ and the efficacy of these barriers $\{E(PB_k)\}$.

The next stage of the process is a comprehensive evaluation of resistance, robustness and resilience of the system to the exposure, the estimation of the susceptibility of the analysed system to the disruptive event and the prediction of the consequences of events $\{C(DE_m)\}$ in the form of losses caused by these events. The negative effects of disruptive events $\{C(DE_m)\}$ can and should be minimized by the use of reactive safety barriers $\{RB_n\}$. Thus, the next step is to assess the efficacy of these barriers $\{E(RB_n)\}$ for each of the potentially possible disruptive event $\{DE_m\}$. Subsequent step of algorithm includes the calculation of the system vulnerability $\{V(DE_m)\}$ to each disruptive event $\{DE_m\}$ as the product of the consequence $\{C(DE_m)\}$ and the efficacy of the reactive barriers $\{E(RB_n)\}$.

The final stage of the proposed procedure is to assess the overall risk matrix, taking into consideration all possible scenarios as a consequence of the disruptive events. The entire disruption risk matrix will be expressed as a N-dimensional vector $R = \{P(DE_m); V(DE_m)\}$, where N is the number of possible scenarios $\{TH_j\}$. And finally *the dependability measure* of the investigated system for a time period (t_1, t_2) can be expressed by the formula:

$$D(t_1, t_2) = P\{[P(DE_m) < P_{cr}(DE)] \cap [V(DE_m) < C_{cr}(DE)]\} \quad (4.3)$$

with:

$P_{cr}(DE)$ critical value of disruption frequency,

$C_{cr}(DE)$ critical value of disruption consequences.

Also, the criterion for complex engineered systems dependability justification is based on the concept of operational risk, and is defined as follows:

Dependability measure of a system is the likelihood to avoid disruptions that are more probable and more severe in consequences than it is acceptable for each possible risky scenario.

References

- Abdelzaher T, Kott A (2013) Resiliency and robustness of complex systems and networks. *Adapt, Dyn Resilient Syst* 67:67–86
- Ackoff RL (1971) Towards a system of systems concepts. *Manage Sci* 17:661–671
- Ackoff RL, Magidson J, Addison HJ (2006) *Idealized design: creating an organization's future*. Pearson Education LTD
- Adger WN, Hughes TP, Folke C, Carpenter SR, Rockström J (2005) Social-ecological resilience to coastal disasters. *Science* 309:1036–1039. <https://doi.org/10.1126/science.1112122>
- Adger WN, Eakin H, Winkels A (2009) Nested and teleconnected vulnerabilities to environmental change. *Front Ecol Environ* 7:150–157. <https://doi.org/10.1890/070148>

- Adger WN, Barnett J, Brown K, Marshall N, O'Brien K (2013) Cultural dimensions of climate change impacts and adaptation. *Nat Clim Change* 3:112–117. <https://doi.org/10.1038/nclimate1666>
- Alberts D (2002) Information age transformation, getting to a 21st century military. DOD Command and Control Research Program
- Allen CR, Pope KL, Fontaine JJ (eds) (2011) Adaptive management for natural resources. *J Environ Manage* 92(5):1339–1428
- Anaya VO (2005) How enterprise architectures can support integration. In: IHIS'05 Bremen, Germany
- Anderson R (2008) Security engineering: a guide to build dependable distributed systems. Wiley, Hoboken, New Jersey
- ANSI (2008) ANSI/EIA/TIA-942. Telecommunications infrastructure standard for data centers—Rev. 5
- Aven T (2011) On some recent definitions and analysis frameworks for risk, vulnerability and resilience. *Risk Anal* 31(4):515–522
- Aven T (2015) Implications of black swans to the foundations and practice of risk assessment and management. *Reliab Eng Syst Saf* 134:83–91
- Avizienis A et al (2004) Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans Dependable Secur Comput* 1(1):11–33
- Barthel S, Folke C, Colding J (2010) Social-ecological memory in urban gardens: retaining the capacity for management of ecosystem services. *Glob Environ Change* 20:255–265. <https://doi.org/10.1016/j.gloenvcha.2010.01.00>
- Basel Committee on Banking Supervision (2006a) High-level principles for business continuity. The Joint Forum, August
- Basel Committee on Banking Supervision (2006b) International convergence of capital measurement and capital standards. A revised framework, June
- Beer S (1979) The heart of the enterprise. Wiley, New York, NY
- Beer S (1984) The viable system model: its provenance, development, methodology and pathology. *J Oper Res Soc* 35(1):7–25
- Beer S (1985) Diagnosing the system for organizations. Oxford University Press, Oxford, England
- Berkes F (2007) Understanding uncertainty and reducing vulnerability: lessons from resilience thinking. *Nat Hazards* 41:283–295
- Berkes F, Colding J, Folke C (eds) (2003) Navigating social-ecological systems: building resilience for complexity and change. Cambridge University Press, Cambridge, UK; <http://dx.doi.org/10.1017/cbo9780511541957>
- Bernus P, Nemes L, Schmidt G (2003) Handbook on enterprise architecture, Springer
- Biggs R, Carpenter SR, Brock WA (2009) Turning back from the brink: detecting and impending regime shift in time to avert it. *Proc Natl Acad Sci USA* 106:826–831. <https://doi.org/10.1073/pnas.0811729106>
- Biggs R, Schlüter M, Schoon ML (eds) (2015) Principles for building resilience: sustaining ecosystem services in socialecological systems. Cambridge University Press, Cambridge, UK. <http://dx.doi.org/10.1017/cbo9781316014240>
- Bilal M, Daclin N, Chapurlat V (2014) Collaborative networked organizations as system of systems: a model-based engineering approach. IFIP AICT
- Billaud S, Daclin N, Chapurlat V (2015) Interoperability as a key concept for the control and evolution of the System of Systems (SoS). In: Conference: international workshop on enterprise interoperability (IWEI 2015). https://doi.org/10.1007/978-3-662-47157-9_5, https://www.researchgate.net/publication/279928616_Interoperability_as_a_Key_Concept_for_the_Control_and_Evolution_of_the_System_of_Systems_SoS
- Bishop TJ, Hydosky FE (2009) Corporate resiliency: managing the growing risk of fraud and corruption. Wiley, Hoboken, New Jersey
- Boardman J, Sauser B (2006) System of systems - the meaning of IEEE/SMC. *Int Conf Syst Syst Eng* 118–123

- Boardman J, Sauser B (2008) Systems thinking: coping with 21st century problems. CRC Press/ Taylor & Francis, Boca Raton, FL
- Bosman R (2006) The new supply chain challenge: risk management in a global economy. FM Global, Johnston, RI
- Brosey WD, Neal ER, Marks DF (2001) Grand challenges of enterprise integration, IEEE
- BSI (2003) British standards institution, publicly available specification n. 56. Guide to Business Continuity Management, London
- Bukowski L (2016) System of systems dependability—theoretical models and applications examples. *Reliab Eng Syst Saf* 151:76–92
- Bukowski L, Feliks J (2005) Application of fuzzy sets in evaluation of failure likelihood. In: Proceedings of the 18th international conference on systems engineering. Las Vegas, IEEE CS, pp 170–175
- Bukowski L, Feliks J (2008) Vector conception of technical system's dependability. In: Proceedings of the 19th international conference on systems engineering. Las Vegas, IEEE CS, pp 492–497
- Cacciabue P (2004) Guide to applying human factors methods. Springer, London
- Carney D, Fisher D, Place P (2005) Topics in Interoperability: system-of-systems evolution. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA
- Carpenter S, Walker B, Anderies JM, Abel N (2001) From metaphor to measurement: resilience of what to what? *Ecosystems* 4:765–781
- Carpenter SR, Westley F, Turner MG (2005) Surrogates for resilience of social-ecological systems. *Ecosystems* 8:941–944. <https://doi.org/10.1007/s10021-005-0170-y>
- Carpenter SR, Folke C, Scheffer M, Westley F (2009) Resilience: accounting for the noncomputable. *Ecol Soc* 14(1):13. [online] <http://www.ecologyandsociety.org/vol14/iss1/art13/>
- Carpenter SR, Arrow KJ, Barrett S, Biggs R, Brock WA, Crépin A-S, Engström G, Folke C, Hughes T, Kautsky N, Li CZ, McCarney G, Meng K, Mäler K-G, Polasky S, Scheffer M, Shogren J, Sterner T, Vincent J, Walker B, Xepapadeas A, de Zeeuw A (2012) General resilience to cope with extreme events. *Sustainability* 4:3248–3259. <https://doi.org/10.3390/su4123248>
- Carpenter SR, Brock WA, Folke C, van Nes E, Scheffer M (2015) Allowing variance may enlarge the safe operating space for exploited ecosystems. *Proc Natl Acad Sci USA* 112:14384–14389. <https://doi.org/10.1073/pnas.1511804112>
- Cash DW, Adger W, Berkes F, Garden P, Lebel L, Olsson P, Pritchard L, Young O (2006) Scale and cross-scale dynamics: governance and information in a multilevel world. *Ecol Soc* 11(2):8. <https://doi.org/10.5751/es-01759-110208>
- Chapin FS, Kofinas GP, Folke C (eds) (2009) Principles of ecosystem stewardship: resilience-based natural resource management in a changing world. Springer, New York, USA
- Christopher M, Peck H (2004) Building Resilient Supply Chain. *Int J Logist Manage* 15:1–13
- Christopher M, Peck H (2009) The five principles of supply chain resilience. *Logist Eur* 12:16–21
- Clarvis MH, Bohensky E, Yarime M (2015) Can resilience thinking inform resilience investments? Learning from resilience principles for disaster risk reduction. *Sustainability* 7:9048–9066. <https://doi.org/10.3390/su7079048>
- Cosens BA (2013) Legitimacy, adaptation, and resilience in ecosystem management. *Ecol Soc* 18(1):3. <https://doi.org/10.5751/ES-05093-180103>
- Costella MF, Saurin TA, Guimaraes LB (2009) A method for assessing health and safety management systems from the resilience engineering perspective. *Saf Sci* 47:1056–1067
- Crane TA (2010) Of models and meanings: cultural resilience in social-ecological systems. *Ecol Soc* 15(4):19. <http://www.ecologyandsociety.org/vol15/iss4/art19/>
- Crépin A-S, Biggs R, Polasky S, Troell M, de Zeeuw A (2012) Regime shifts and management. *Ecol Econ* 84:15–22. <https://doi.org/10.1016/j.ecolecon.2012.09.003>
- Cumming GS, Olsson P, Chapin FS, Holling CS (2013) Resilience, experimentation, and scale mismatches in social-ecological landscapes. *Landsc Ecol* 28:1139–1150. <https://doi.org/10.1007/s10980-012-9725-4>

- Cummins FA (2002) *Enterprise Integration: an architecture for enterprise application and systems integration*. Wiley Inc
- Dakos V, Scheffer M, van Nes EH, Brovkin V, Petoukhov V, Held H (2008) Slowing down as an early warning signal for abrupt climate change. *Proc Natl Acad Sci USA* 105:14308–14312. <https://doi.org/10.1073/pnas.0802430105>
- Dalziell EP, McManus ST (2004) Resilience, vulnerability, adaptive capacity: implications for system performance. In: *International forum for engineering decision making (IFED) stoos*, Switzerland
- de Leeuw A, Volberda H (1996) On the concept of flexibility: a dual control perspective. *Omega Int J Manage Sci* 24:121–139
- de Weck OL, Roos D, Magee CL (2011) *Engineering systems: meeting human needs in a complex technological world*. MIT Press, Cambridge, MA
- Dekker S et al (2008) *Resilience engineering: new directions for measuring and maintaining safety in complex systems*. Final Report December 2008
- Deloitte (2018) *Business continuity management. Towards a Resilient Organisation*. <https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-risk-bcm-resilient-organisation.pdf>
- Díaz S, Quétier F, Cáceres DM, Trainor SF, PérezHarguindeguy N, Bret-Harte MS, Finegan B, Peña-Claros M, Poorter L (2011) Linking functional diversity and social actor strategies in a framework for interdisciplinary analysis of nature's benefits to society. *Proc Natl Acad Sci USA* 108:895–902. <https://doi.org/10.1073/pnas.1017993108>
- 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
- DTN (2012) *Delay and disruption tolerant networks (DTNs) a tutorial*, Version 2.0. http://DTN_Tutorial_v2.04.pdf
- Ebbesson J (2010) The rule of law in governance of complex socioecological changes. *Glob Environ Change* 20:414–422. <https://doi.org/10.1016/j.gloenvcha.2009.10.009>
- Ebbesson J, Hey E (2013) Introduction: where in law is social-ecological resilience? *Ecol Soc* 18 (3):25. <https://doi.org/10.5751/ES-05750-180325>
- Eisner H (1993) RCASSE: rapid computer-aided system of systems engineering. In: *Proceedings of 3rd international symposium of the national council of systems engineering*, vol 1, Washington, DC, pp 267–273
- Elmqvist T, Folke C, Nyström M, Peterson G, Bengtsson J, Walker B, Norberg J (2003) Response diversity, ecosystem change, and resilience. *Front Ecol Environ* 1:488–494. [http://dx.doi.org/10.1890/1540-9295\(2003\)001\[0488:RDECAR\]2.0.CO;2](http://dx.doi.org/10.1890/1540-9295(2003)001[0488:RDECAR]2.0.CO;2)
- El-Thalji I (2011) *System dependability engineering for wind power application*. <http://www.diva-portal.org/smash/get/diva2:443903/fulltext01>
- Erl T (2007) *SOA principles of service design*. Prentice Hall
- Erol O, Henry D, Sauser B, Mansouri M (2010) Perspectives on measuring enterprise resilience. <https://www.researchgate.net/publication/224144529>
- Fiksel J (2006) Sustainability and resilience: toward a systems approach. *Sustain Sci Pract Policy* 2:14–21
- Folke C (2016) Resilience. In: Shugart H (Editor-in-Chief) *Framing concepts in environmental science*. Oxford research encyclopedias, environmental science. Oxford University Press, New York. <http://dx.doi.org/10.1093/acrefore/9780199389414.013.8>
- Folke C, Chapin III FS, Olsson P (2009) Transformations in ecosystem stewardship. In: Folke C, Kofinas GP, Chapin III FS (eds) *Principles of ecosystem stewardship: resilience-based natural resource management in a changing world*. Springer, New York, New York, USA, pp 103–125. <http://dx.doi.org/10.1007/978-0-387-73033-25>
- Folke C, Colding J, Berkes F (2003) Synthesis: building resilience and adaptive capacity in social-ecological systems 352–387. In: Berkes F, Colding J, Folke C (eds) *Navigating social-ecological systems: building resilience for complexity and change*. Cambridge University Press, Cambridge, UK, pp 352–387. <http://dx.doi.org/10.1017/cbo9780511541957.020>

- Folke C, Hahn T, Olsson P, Norberg J (2005) Adaptive governance of social-ecological systems. *Annu Rev Environ Resour* 30:441–473. <http://dx.doi.org/10.1146/annurev.energy.30.050504.144511>
- Folke C, Carpenter SR, Walker BH, Scheffer M, Chapin III FS, Rockström J (2010) Resilience thinking: integrating resilience, adaptability and transformability. *Ecol Soc* 5(4):20. [online] <http://www.ecologyandsociety.org/vol15/iss4/art20/>
- Frankel AS, Leonard MW, Denham CR (2006) Fair and just culture, team behaviour, and leadership engagement: the tools to achieve high reliability. *Health Serv Res* 41(4):1690–1709
- Fricke E, Schulz AP (2005) Design for changeability (DfC): principles to enable changes in systems throughout their entire lifecycle. *Syst Eng J* 8:342–359
- Gallopín GC (2006) Linkages between vulnerability, resilience, and adaptive capacity. *Glob Environ Change* 16:293–303
- Garmestani AS, Allen CR, Benson MH (2013) Can law foster social-ecological resilience? *Ecol Soc* 18(2):37. <https://doi.org/10.5751/ES-05927-80237>
- Giachero A, Giordano F, Schiraldi MM (2013) From business continuity to design of critical infrastructures: ensuring the proper resilience level to datacentres. *Int J Eng Technol* 5(4):3544–3553
- Gibbs MT (2009) Resilience: what is it and what does it mean for marine policymakers? *Mar Policy* 33:322–331
- Gisladottir V, Ganin AA, Keisler JM, Kepner J, Linkov I (2017) Resilience of cyber systems with over- and underregulation. *Risk Anal* 37(9):1644–1651
- Goble G, Fields H, Cocchiara R (2002) Resilient infrastructure. IBM Global Services, September
- Goethals F, Vandenbulcke J, Lemahieu W (2004) Developing the extended enterprise with the FADEE. In: 2004 ACM symposium on applied computing Nicosia, Cyprus
- Goulden MC, Adger WN, Allison EH, Conway D (2013) Limits to resilience from livelihood diversification and social capital in lake social-ecological systems. *Ann Assoc Am Geogr* 103:906–924. <https://doi.org/10.1080/00045608.2013.765771>
- Gunderson LH, Holling CS (eds) (2002) *Panarchy: understanding transformations in human and natural systems*. Island, Washington, D.C., USA
- Gunderson LH, Holling CS, Light SS (eds) (1995) *Barriers and bridges to the renewal of ecosystems and institutions*. Columbia University Press, New York, New York, USA
- Haimes YY, Crowther K, Horowitz BM (2008) Homeland security preparedness: balancing protection with resilience in emergent systems. *Syst Eng* 11:287–308
- Hall PA, Lamont M (eds) (2013) *Social resilience in the neoliberal era*. Cambridge University Press, New York, USA
- Hasselbring W (2000) Information system integration, association for computing machinery. *Commun ACM* 43:32–38
- Helaakoski H, Iskanius P, Peltomaa I (2007) Agent-based architecture for virtual enterprises to support agility. In: Camarinha-Matos L, Afsarmanesh H, Novais P, Analide C (eds) *Establishing the foundation of collaborative networks*, vol. 243. Springer, Boston, pp 299–306
- Hester PT (2012) Why optimisation of a system of systems is both unattainable and unnecessary. *Int J Syst Syst Eng* 3(3/4):268–276
- Hill M, Engle NL (2013) Adaptive capacity: tensions across scales. *Environ Policy Governance* 23:177–192. <https://doi.org/10.1002/eet.1610>
- Holling CS (1986) The resilience of terrestrial ecosystems: local surprise and global change. In: Clark WC, Munn RE (eds) *Sustainable development of the biosphere*. Cambridge University Press, Cambridge, UK, pp 292–317
- Hollnagel E (2009) The four cornerstones of resilience engineering. In: Nemeth C, Hollnagel E, Dekker S (eds) *Resilience engineering perspectives: preparation and restoration*, vol 2. Ashgate, Burlington, pp 117–133
- Hollnagel E, Woods DW, Leveson N (eds) (2006) *Resilience engineering: concepts and precepts*. Ashgate, Abingdon, Oxon, GBR

- Homer-Dixon T, Walker B, Biggs R, Crépin A-S, Folke C, Lambin EF, Peterson GD, Rockström J, Scheffer M, Steffen W, Troell M (2015) Synchronous failure: the emerging causal architecture of global crisis. *Ecol Soc* 20(3):6. <https://doi.org/10.5751/es-07681-200306>
- Hopkins A (2007) The problem of defining high reliability organisations. Working Paper 51. The Australian National University
- Horne JF (1997) The coming age of organizational resilience. *Bus Forum* 22–24. http://www.cit.iit.bas.bg/cit_2013/v13-2/10341-volume13_issue_2-01_paper.pdf
- Hu Y, Li J, Holloway EL (2008) Towards modeling of resilience dynamics in manufacturing enterprises: literature review and problem formulation. In: 4th IEEE conference on automation science and engineering Washington DC: IEEE, pp 279–284
- Huang A, Yen DC, Chou DC, Xu Y (2003) Corporate applications integration: challenges, opportunities, and implementation strategies. *J Bus Manage* 9:37–150
- Hughes TP, Linares C, Dakos V, van de Leemput IA, van Nes EH (2013) Living dangerously on borrowed time during slow, unrecognized regime shifts. *Trends Ecol Evol* 28:149–155. <https://doi.org/10.1016/j.tree.2012.08.022>
- IBM (2005) The solution designer's guide to IBM on demand business solutions. IBM 2005
- IEEE 610.12 (1990) Standard glossary of software engineering terminology. International Organization for Standardization and IEEE, NY
- IEEE-Std-1471 (2000) Recommended practice for architectural description of software-intensive systems, IEEE 2000
- IEC (2015) International standards on dependability, The world's online electrotechnical vocabulary. <http://www.electropedia.org/>
- Institute for Risk Management (2015) <http://www.ey.com/Publication/vwLUAssets/EY-rethinking-risk-management/%24FILE/EY-rethinking-risk-management.pdf>
- Irani Z, Themistocleous M, De Love PE (2003) The impact of enterprise application integration on information system lifecycles. *Inf Manage* 41:177–187
- ISO (2005) ISO 27005:2008 Information technology—security techniques—information security risk management. <https://www.iso.org/standard/42107.html>
- ISO/IEC 27005 (2008) Information technology—security techniques—information security risk management. http://www.pqm-online.com/assets/files/lib/std/iso_iec_27005-2008.pdf
- Jamshidi M (2005) System-of-systems engineering—a definition. In: IEEE international conference on system, man and cybernetics (SMC), Waikoloa, Hawaii, vol 4, Oct 2005, pp 10–12. http://ieeemc2005.unm.edu/SoSE_Defn.htm
- Jamshidi M (ed) (2008) System of systems engineering: innovations for the 21st century. Hoboken, NJ, John Wiley
- Jamshidi M (2011) System of systems engineering: innovations for the twenty-first century. Wiley
- Jansson Å, Polasky S (2010) Quantifying biodiversity for building resilience for food security in urban landscapes: getting down to business. *Ecol Soc* 15(3):20. <http://www.ecologyandsociety.org/vol15/iss3/art20/>
- Kaāniche M, Laprie JC, Blanquart JP (2000) Dependability engineering of complex computing systems. In: 6th international conference on engineering of complex computer systems (ICECCS 2000), Tokyo, Japan. http://homepages.laas.fr/kaaniche/Slides/Pres_ICECCS%2700.pdf
- Kasunic M (2004) Measuring systems interoperability: challenges and opportunities. Tech. Note C. 2004 TN 003 Carnegie-Mellon Univ Pittsburgh PA Softw. Eng. INST
- Kates RW, Clark WC (1996) Environmental surprise: expecting the unexpected? *Environment* 38:6–34. <https://doi.org/10.1080/00139157.1996.9933458>
- Keating C (2005) Research foundations for system of systems engineering. In: IEEE international conference on systems, man and cybernetics, Waikoloa, Hawaii, Oct 2005, pp 2720–2725
- Keating C, Katina P (2016) Complex system governance development: a first generation methodology. *Int J Syst Syst Eng* 7(1/2/3):43–74
- Keating CB, Morin M (2001) An approach for systems analysis of patient care operations. *J Nurs Adm* 31(7/8):355–363
- Keating C, Rogers R, Unal R, Dryer D, Sousa-Poza A, Safford R, Peterson W, Rabadi G (2003) System of systems engineering. *Eng Manage J* 15(3):36–45

- Keating CB, Katina PF, Bradley JM (2014) Complex system governance: concept, challenges, and emerging research. *Int J Syst Syst Eng* 5(3):263–288
- Kleindorfer PR, Saad GH (2005) Managing disruption risks in supply chains. *Prod Oper Manag* 14 (1):53–68
- Koch BA (1993) Differentiating reliability-seeking organisations from other organisations: development and validation of an assessment device. In: Roberts KH (ed) *New challenges to understanding organizations*. Macmillan, New York, pp 75–97
- Kosanke K, Nell JG (1997) *Enterprise engineering and integration: building international consensus*. Springer, Berlin
- Kosanke K, Vernadat F, Zelm M (1999) CIMOSA: enterprise engineering and integration. *Comput Ind* 40:83–97
- Kröger W, Zio E (2011) *Vulnerable systems*. Springer, London
- Kühnle H, Wagenhaus G (2005) Extended enterprise architectures (E2A)—towards a powerful mode of production
- Lam W (2005) Investigating success factors in enterprise application integration: a case-driven analysis. *Eur J Inf Syst* 14:175–187
- Lambin EF, Meyfroid P (2011) Global land use change, economic globalization, and the looming land scarcity. *Proc Nat Acad Sci USA* 108:3465–3472. <https://doi.org/10.1073/pnas.1100480108>
- Lebel L, Anderies JM, Campbell B, Folke C, HatfieldDodds S, Hughes TP, Wilson J (2006) Governance and the capacity to manage resilience in regional social-ecological systems. *Ecol Soc* 11(1):19. <https://doi.org/10.5751/es-01606-110119>
- Lekka C (2011) High reliability organisations a review of the literature. RR899 Research Report; <http://www.hse.gov.uk/research/rrpdf/rr899.pdf>
- Leveson N (2008) System safety engineering: back to the future. <http://sunnyday.mit.edu/book2.html>
- Levin S, Xepapadeas T, Crépin A-S, Norberg J, de Zeeuw A, Folke C, Hughes TP, Arrow K, Barrett S, Daily G, Ehrlich P, Kautsky N, Mäler K-G, Polasky S, Troell M, Vincent J, Walker BH (2013) Social-ecological systems as complex adaptive systems: modeling and policy implications? *Environ Dev Econ* 18:111–132. <https://doi.org/10.1017/S1355770X12000460>
- Linkov I, Eisenberg D, Plourde K et al (2013) Resilience metrics for cyber systems. *Environ Syst Decis* 33(4):471–476. <https://doi.org/10.1007/s10669-013-9485-y>
- Linkov I, Bridges T, Creutzig F (2014) Changing the resilience paradigm. *Nat Clim Chang* 4 (6):407–409. <https://doi.org/10.1038/nclimate2227>
- Lyon C (2014) Place systems and social resilience: a framework for understanding place in social adaptation, resilience, and transformation. *Soc Nat Resour* 27:1009–1023. <https://doi.org/10.1080/08941920.2014.918228>
- Madsen P, Desai V, Roberts K, Wong D (2006) Mitigating hazards through continuing design: the birth and evolution of a paediatric intensive care unit. *Organ Sci* 17(2):239–248
- Maier MW (1998) Architecting principles for systems-of-systems. *Syst Eng* 1(4):267–284
- Mallak L (1998) Putting organizational resilience to work. *Ind Manage* 40:8–13
- Mallak L (1999) Toward a theory of organizational resilience. In: Portland international conference on technology and innovation management. PICMET, vol 1, p 223
- Manyena SB (2006) The concept of resilience revisited. *Disasters* 30:434–450
- Marshall NA, Park SE, Adger WN, Brown K, Howden SM (2012) Transformational capacity and the influence of place and identity. *Environ Res Lett* 7:034022. <https://doi.org/10.1088/1748-9326/7/3/034022>
- Masten AS (2015) Resilience in human development: Interdependent adaptive systems in theory and action. <http://www.resilienceresearch.org/files/PTR/AnnMasten-PTRKeynote.pdf>
- McDaniels T, Chang SE, Cole D, Mikawoz J, Longstaff H (2008) Fostering resilience to extreme events within infrastructure systems: characterizing decision contexts for mitigation and adaptation. *Glob Environ Change* 18(2):310–318

- MIIB (2008) Major incident investigation board. The Buncefield incident 11 Dec 2005. The final report of the Major Incident Investigation Board, vol 1. <http://www.buncefieldinvestigation.gov.uk/reports/volume1.pdf> Accessed on
- Morello D (2001) The blueprint for the resilient virtual organization, Gartner Jan 2001
- NAS (2012) Disaster resilience: a national imperative. National Academy of Sciences (US)
- Nelson DR, Adger WN, Brown K (2007) Adaptation to environmental change: contributions of a resilience framework. *Annu Rev Environ Resour* 32:395–419. <https://doi.org/10.1146/annurev.energy.32.051807.090348>
- NFPA (2013) National fire protection association 1600: standard on disaster/emergency management and business continuity programs. Quincy, Massachussets, US
- Österblom H, Jouffray J-B, Folke C, Crona B, Troell M, Merrie A, Rockström J (2015) Transnational corporations as keystone actors in marine ecosystem. *PLoS ONE* 10(5): e0127533. <https://doi.org/10.1371/journal.pone.0127533>
- Ostrom E (1990) Governing the commons: the evolution of institutions for collective actions. Cambridge University Press, New York, USA. <http://dx.doi.org/10.1017/CBO9780511807763>
- Ostrom E (2007) A diagnostic approach for going beyond panaceas. *Proc Natl Acad Sci USA* 104:15181–15187. <https://doi.org/10.1073/pnas.0702288104>
- Pahl-Wostl C, Lebel L, Knieper C, Nikitina E (2012) From applying panaceas to mastering complexity: toward adaptive water governance in river basins. *Environ Sci Policy* 23:24–34. <https://doi.org/10.1016/j.envsci.2012.07.014>
- Panetto H (2006) Meta-modèles et modèles pour l'intégration et l'interopérabilité des applications d'entreprises de production. Dr. Diss. Univ. Henri Poincaré-Nancy I
- Park J, Seager TP, Rao PSC, Convertono M, Linkov I (2013) Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Anal* 33(3):356–367
- Patterson ES, Woods DD, Cook RI, Render ML (2007) Collaborative cross-checking to enhance resilience. *Cogn Tech Work*, pp 155–162
- Perrow C (1984) Normal accidents: living with high-risk technologies. Basic Books, New York
- Perrow C (1994) The limits of safety: the enhancement of a theory of accidents. *J Contingencies Cris Manage* 2(4):212
- Petrie CJ (1992) Enterprise integration modeling. The MIT Press, Cambridge
- Pierce WH (1965) Failure-tolerant computer design. Academic Press, Paris
- Plieninger T, Bieling C (eds) (2012) Resilience and the cultural landscape: understanding and managing change in humanshaped environments. Cambridge University Press, Cambridge, UK. <https://doi.org/10.1017/cbo9781139107778>
- Polasky S, de Zeeuw A, Wagener F (2011) Optimal management with potential regime shifts. *J Environ Econ Manage* 62:229–240. <https://doi.org/10.1016/j.jeem.2010.09.004>
- Provera B, Montefusco A, Canato A (2008) A 'no blame' approach to organizational learning. *Br J Manage*. <https://doi.org/10.1111/j.1467-8551.2008.00599.x>
- PSA (2004) Petroleum safety authority Norway. HSE and culture. <http://www.ptil.no/getfile.php/z%20Konvertert/Products%20and%20services/Publications/Dokumenter/hescultureny.pdf>
- PSA (2010) Petroleum safety authority Norway. Safety—Status and Signals 2009–2010. <http://www.ptil.no/news/new-publication-safety-status-and-signals-2009-2010-article658079.html>
- Quinlan AE, Barbés-Blázquez M, Haider LJ, Peterson GD (2015) Measuring and assessing resilience: broadening understanding through multiple disciplinary perspectives. *J Appl Ecol* 23:677–687. <https://doi.org/10.1111/1365-664.12550>
- Raut A, Basavaraja A (2003) Enterprise business process integration. In: TENCON 2003: conference on convergent technologies for AsiaPacific region, pp 1549–1553
- Reason J (2000) Human error: models and management. *BMJ* 320:768770
- Reason J (2005) Safety culture: some theoretical and practical issues. In: Morray N (ed) *Ergonomics major writings: the history and scope of human factors*, vol 1. Taylor and Francis, Oxon
- Reason J (2008) The human contribution: unsafe acts, accidents and heroic recoveries. Ashgate, Surrey, England

- Reyers B, Biggs R, Cumming GS, Elmqvist T, Hejnowicz AP, Polasky S (2013) Getting the measure of ecosystem services: a social-ecological approach. *Front Ecol Environ* 11:268–273. <https://doi.org/10.1890/120144>
- Richey RG, Natarajaratnam M, Capar I, Narayanan A (2009) Managing supply chains in times of crisis: a review of literature and insights. *Int J Phys Distrib Logist Manag* 39(7):535–573
- Rittel HW, Webber MM (1973) Dilemmas in a general theory of planning. *Policy Sci* 4(2):155–169
- Roberts K (1990) Some characteristics of one type of high reliability organisation. *Organ Sci* 1 (2):160–176
- Roberts KH, Bea R (2001) Must accidents happen? Lessons from high-reliability organisations. *Acad Manage Exec* 15(3):70–79
- Roberts K, Rousseau DM (1989) Research in nearly failure-free, high reliability organisations: having the bubble. *IEEE Trans Eng Manage* 36(2):132139
- Rockström J, Steffen W, Noone K, Persson Å, Chapin FS III, Lambin EF, Lenton TM, Scheffer M, Folke C, Schellnhuber HJ, Nykvist B, de Wit CA, Hughes T, van der Leeuw S, Rodhe H, Sörlin S, Snyder PK, Costanza R, Svedin U, Falkenmark M, Karlberg L, Corell RW, Fabry VJ, Hansen J, Walker BH, Liverman D, Richardson K, Crutzen P, Foley JA (2009) A safe operating space for humanity. *Nature* 461:472–475. <https://doi.org/10.1038/461472a>
- Rockström J, Falkenmark M, Folke C, Lannerstad M, Barron J, Enfors E, Gordon L, Heinke J, Hoff H, Pahl-Wostl C (2014) Water resilience for human prosperity. Cambridge University Press, Cambridge, UK. <http://dx.doi.org/10.1017/CBO9781139162463>
- Rouse WB (2005) Enterprises as systems: essential challenges and approaches to transformation. *Syst Eng J* 8:138–150
- Sage AP, Cuppan CD (2001) On the systems engineering and management of systems and federations of systems. *Inf Knowl Syst Manage* 2(4):325–345
- Scheffer M, Carpenter SR, Lenton TM, Bascompte J, Brock W, Dakos V, van de Koppel J, van de Leemput IA, Levin SA, van Nes EH, Pascual M, Vandermeer J (2012) Anticipating critical transitions. *Science* 338:344–348. <https://doi.org/10.1126/science.1225244>
- Scheffer M, Barrett S, Carpenter S, Folke C, Greene AJ, Holmgren M, Hughes TP, Kosten S, van de Leemput I, Nepstad D, van Nes EH, Peeters ETHM, Walker BH (2015) Creating a safe operating space for iconic ecosystems. *Science* 347:1317–1319. <https://doi.org/10.1126/science.aaa3769>
- Schill C, Lindahl T, Crépin A-S (2015) Collective action and the risk of ecosystem regime shifts: insights from a laboratory experiment. *Ecol Soc* 20(1):48. <https://doi.org/10.5751/es-07318-200148>
- Scholes RJ, Reyers B, Biggs R, Spierenburg MJ, Duriappah A (2013) Multi-scale and cross-scale assessments of social-ecological systems and their ecosystem services. *Curr Opin Environ Sustain* 5:16–25. <https://doi.org/10.1016/j.cosust.2013.01.004>
- Scott M, Sorcinelli G, Gutierrez P, Moffatt C, DesAutels P (2006) CONFERENCEXP: an enabling technology for organizational resilience. In: Donnellan B, Larsen T, Levine L, D. J (eds) *The transfer and diffusion of information technology for organizational resilience*, vol 206. Springer, Boston, pp 219–227
- Shafieezadeh A, Burden LI (2014) Scenario-based resilience assessment framework for critical infrastructure systems: case study for seismic resilience of seaports. *Reliab Eng Syst Saf* 132:207–219
- Sheffi Y (2007) *The resilient enterprise: overcoming vulnerability for competitive advantage*. MIT Press, Cambridge
- Sheffi Y, Rice JB Jr (2005) A supply chain view of the resilient enterprise. *MIT Sloan Management Review* 47(1):41–48
- SIoT—Stevens Institute of Technology (2006) *Castle point on Hudson*, Hoboken, N. 07030: Report on system of systems engineering
- Smith D, O'Brien L, Kontogiannis K, Barbacci M (2002) *Enterprise integration, architect (SEI Interactive News)*, vol 4Q
- Stead E, Smallman C (1999) Understanding business failure: learning and un-learning lessons from industrial crises. *J Contingencies Cris Manage* 7(1):1–18

- Steffen W, Richardson K, Rockström J, Cornell S, Fetzer I, Bennett E, Biggs R, Carpenter SR, de Vries W, de Wit CA, Folke C, Gerten D, Heinke J, Mace GM, Persson LM, Ramanathan V, Rayers B, Sörlin S (2015) Planetary boundaries: guiding human development on a changing planet. *Science* 347(6223). <http://dx.doi.org/10.1126/science.1259855>
- Stephans RA (2004) *System safety for the 21st century*. Wiley-Interscience, Hoboken, New Jersey
- Stevenson M, Spring M (2007) Flexibility from a supply chain perspective: definition and review. *Int J Oper Prod Manage* 27:2007
- Stohr EA, Nickerson JV (2003) Intra enterprise integration: methods and direction. In: Luftman J (ed) *Competing in the information age*. Oxford University Press, New York
- Straube F, Pfohl HC (2009) *Global networks in an era of change*. Environment, Security, Internationalization, People, Hamburg
- Sushil (2006) Enterprise flexibility, global. *J Flex Syst Manage* 2:53–58
- Sutcliffe KM (2003) Organizing for resilience. In: Cameron KS, Dutton IE, Quinn RE (eds) *Positive organizational scholarship*. Berrett-Koehler, San Francisco, pp 94–110
- Taleb NN (2007) *The black swan: the impact of the highly improbable*. London: Penguin
- Taleb NN (2012) *Anti fragile: things that gain from disorder*. London: Penguin
- Tamuz M, Harrison MI (2006) Improving safety in hospitals: contributions of high reliability theory and normal accident theory. *Health Res Educ Trust* 41(4):1654–1673
- Themistocleous M, Corbitt G (2006) Is business process integration feasible? *J Enterp Inf Manage* 19:434–449
- Tidball KG, Krasny ME, Svendsen E, Campbell L, Helphand K (2010) Stewardship, learning, and memory in disaster resilience. *Environ Educ Res* 6:591–609. <https://doi.org/10.1080/13504622.2010.505437>
- Tzanev A (2013) Modeling and simulation of systems of systems—a survey
- Ungar M (2016) The resilience research centre adult resilience measure (RRC-ARM); user's manual. <http://www.resilienceresearch.org/files/CYRM/Adult%20-%20CYRM%20Manual.pdf>
- Ungar M, Liebenberg L (2011) Assessing resilience across cultures using mixed methods: construction of the child and youth resilience measure. *J Mix Methods Res* 5(2):126–149
- Vancoppenolle G (2007). What are we planning for? In: Hiles A (ed) *The definitive handbook of business continuity management*, 2nd edn. Wiley Ltd
- Venkatachalam AR (2006) A Holistic perspective on enterprise integration. *J Inf Technol Case Appl Res* 8:1–6
- Vernadat FB (1996) *Enterprise modeling and integration: principles and applications*. Chapman & Hall, London
- Vogus TJ, Sutcliffe K (2007a) The safety organising scale: development and validation of a behavioural measure of safety culture in hospital nursing units. *Med Care* 45(1):4654
- Vogus TJ, Sutcliffe KM (2007b) Organizational resilience: towards a theory and research agenda. In: *Systems, man and cybernetics*
- Walker B et al (2002) Resilience management in social-ecological systems: a working hypothesis for a participatory approach. *Conserv Ecol* 6:14–31
- Walker B, Holling CS, Carpenter SR, Kinzig A (2004) Resilience, adaptability and transformability in social-ecological systems. *Ecol Soc* 9(2):5. <https://doi.org/10.5751/es-00650-090205>
- Walker BH, Abel N, Anderies JM, Ryan P (2009) Resilience, adaptability, and transformability in the Goulburn Broken Catchment, Australia. *Ecol Soc* 14(1):12. [online] <http://www.ecologyandsociety.org/vol14/iss1/art12/>
- Waters D (2007) *Supply chain risk management: vulnerability and resilience in logistics*. Kogan Page Limited, London & Philadelphia
- Weick KE, Sutcliffe KM (1997) *Managing the unexpected: resilient performance in an age of uncertainty*. Hoboken: John Wiley and Sons
- Weick KE, Sutcliffe KM (2001) *Managing the unexpected*. Jossey-Bass, San Francisco
- Weick KE, Sutcliffe KM (2007) *Managing the unexpected: resilient performance in an age of uncertainty*, 2nd edn. Jossey-Bass, San Francisco

- Weick KE, Sutcliffe KM, Obstfeld D (1999) Organizing for high reliability: processes of collective mindfulness. In: Sutton RS, Staw BM (eds) *Research in organizational behavior*, vol 1. Jai Press, Stanford, pp 81–123
- Westley F, Olsson P, Folke C, Homer-Dixon T, Vredenburg H, Loorbach D, Thompson J, Nilsson M, Lambin E, Sendzimir J, Banarjee B, Galaz V, van der Leeuw S (2011) Tipping towards sustainability: emerging pathways of transformation. *Ambio* 40:762–780. <https://doi.org/10.1007/s13280-011-0186-9>
- Westrum R (2006) A typology of resilience situations. In: Hollnagel E, Woods DD, Leveson N (eds) *Resilience engineering: concepts and precepts*. Ashgate Press, Aldershot, UK, pp 49–60
- Wreathall J (2006) Properties of resilient organisations: an initial view. In: Hollnagel E, Woods DD, Levenson N (eds) *Resilience engineering: concepts and precepts*. Ashgate, Hampshire, pp 275–285
- Yang HM, Lu FV (2005) Integrating inter- and extra-enterprise applications using web services. *Rev Bus* 26:3–9
- Young OR, Berkhout F, Gallopin GC, Janssen MA, Ostrom E, van der Leeuw S (2006) The globalization of socioecological systems: an agenda for scientific research. *Glob Environ Change* 16:304–316. <https://doi.org/10.1016/j.gloenvcha.2006.03.004>
- Zachman J (1987) A framework for information systems architecture. *IBM Syst J* 26
- Zhu J, Tian Z, Li T, Sun W, Ye S, Ding W, Wang CC, Wu G, Weng L, Huang S, Liu B, Chou D (2004) Model-driven business process integration and management: a case study with the Bank SinoPac regional service platform. *IBM J Res Dev* 48:649–669
- Zio E (2007) From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures. *Inter J Crit Infra* 3(3/4):488
- Zio E (2009) Reliability engineering: old problems and new challenges. *Reliab Eng Syst Saf* 94 (2):125–141

Chapter 5

Modelling and Simulation of Logistic Networks



Learning by doing, peer-to-peer teaching, and computer simulation are all part of the same equation.

Nicholas Negroponte

5.1 Modelling and Simulation of Complex Engineered Systems

5.1.1 Main Principles of Modelling and Simulation

The term ‘model’ refers to an abstract representation of the reality. The use of models (in particular, mathematical ones) as a basis for analysis and reasoning is well established in many scientific and practical disciplines. The widespread availability of computing power makes the experimentation with complex models possible and hence, the emergence of the modelling and simulation as a new research field. There is a strong connection between the model that is appropriate for the investigation and the nature of the problem that should be solved. However, there rarely exists the universal model which will support all modelling and simulation projects that have a common system context. This is especially true when the system has a high level of complexity. Identification of the most appropriate model for complex engineered systems is usually the most challenging aspect of the modelling and simulation approach to problem solving.

The phrase ‘modelling and simulation’ (M&S) have a generally accepted meaning and implies two distinct activities. The modelling activity creates a model which is subsequently used as a an object for experimentation. This experimentation with the model is the simulation activity. Unfortunately, the wide-ranging and essentially inconsistent usages of the word ‘simulation’ can cause regrettable confusion and misunderstandings. We will avoid such multiplicity of uses of this term and use it only in the main sense.

A model plays the role of a surrogate for the system, and represents its characteristics (attributes) in experimental studies. When the underlying system does not yet exist (e.g., it is an idea, concept, or proposal) then the model is the only option

for experimentation. But even when the real system exists there is a variety of reasons why experimenting directly with it could be inappropriate. For example, such experimentation might be (Birta and Arbez 2007):

- Too costly (e.g. determining the performance benefit by upgrading the system at all the nodes of a large communications network);
- Too dangerous (e.g. if operational events pose a serious safety risk);
- Too time-consuming (e.g. investigation of slowly occurring changes);
- Too disruptive (e.g. cascading failures);
- Ethically unacceptable (e.g. experiments on people and their feelings);
- Irreversible (e.g. investigating the impact of a fiscal policy change on the economy of a country).

A typical model is a specification for system behaviour generation and the modelling process is focused on the development of this specification. The goal of this process is to ensure that the behaviour of the model will be as similar as possible to the behaviour of the real system as well as reproducibility of investigation results. The main challenge is to capture all relevant detail and to avoid superfluous features, which is in line with the well-known quotation from Albert Einstein, ‘Everything should be made as simple as possible, but not simpler.’

Modelling is a constructive activity whose goal is to build a sufficiently good model. Usually, a key question is whether the model is good enough from the point of view of the project goals. It means that it is not meaningful to undertake any modelling study without a clear understanding of the purpose for which the model will be used. There is a variety of ways in which the specification of behaviour can be formulated, for example: natural language, mathematical formalisms, rule-based formalisms, symbolic or graphical descriptions, and combinations of these. A particular format that plays a very important role is a specification formulated as a computer program, because computer programs provide the means for carrying out the experiments that are central to the modelling and simulation approach. This illustrates the fact that some realisations of the specification are actually executable and produce the behaviour we want to observe.

However, like other methods, modelling and simulation has some weaknesses, and must be used with care and wisdom. Below are some reasons why modelling and simulation projects can fail (Birta and Arbez 2007):

- Inappropriate statement of goals. No project can ever be successful unless its objectives are clearly articulated and fully understood by all the stakeholders. Ambiguity in the statement of goals can lead to wasted effort or yield conclusions that are unrelated to the objective of the project. The project goals have to be consistent with the maturity of knowledge that characterises the modelled system, as well as the available level of resources (e.g. time, skills, equipment, etc.) should be adequate to achieve the goals.
- Inappropriate granularity of the model. The granularity of the model refers to the level of detail (the degree of resolution) with which it attempts to replicate the system. The level of granularity is necessarily bounded by the goals of

the project. Excessive detail increases complexity and this can lead to cost overruns and/or completion delays that usually translate into project failure. However, too little detail can mask the very effects that have substantial relevance to the behaviour of the modelled system.

- Ignoring unexpected behaviour. Although a validation process is recognised to be an essential stage in any modelling and simulation project, its main thrust is to confirm that expected behaviour does occur. Such behaviour can sometimes occur and when it is observed there often is a tendency to dismiss it, particularly when validation tests have provided satisfactory results. Ignoring such counterintuitive observations can be the foundation for failure.
- Inappropriate combination of essential skills. A modelling and simulation project have substantial requirements in terms of both the range of skills and the effort needed for its completion. Team members contribute complementary expertise to the intrinsically multifaceted requirements of the project. The range of skills that needs to be represented among the team members can include: project management, documentation, using domain knowledge for building dynamic model, experiment design, software development, and analysis of results. The intensity of coverage of these various areas is dependent on the specific nature of the project. Nevertheless, an inappropriate mix of skills can ultimately result in project failure.
- Inadequate flow of information. It is necessary to ensure permanent and correct flow of information between all team members who implement the project. For example, a minor misinterpretation of requirements can have consequences that can lead to the failure of the entire project.

The typical simulation model consists of the following components: system entities, input variables, performance measures, and functional relationships. Almost all simulation software packages provide constructs to model each of the above components. Modelling is regarded as the most important part of a simulation study, because a simulation study can be only as good as the simulation model. Full simulation process comprises the following eleven steps (Maria 1997):

Step 1. *Identify the problem.* Enumerate problems with an existing system and produce requirements for a proposed system.

Step 2. *Formulate the problem.* Select the boundaries of the system to be studied and define overall objective of the study as well as some specific issues to be addressed. Define quantitative criteria on the basis of which different system configurations will be compared and ranked. Identify briefly the configurations of interest and formulate hypotheses about system performance. Decide the time frame of the study and identify the end user of the simulation model. All these problems have to be formulated as precisely as possible.

Step 3. *Collect and process real system data.* Gather data on system specifications, input variables, as well as performance of the existing system. Identify sources of uncertainty in the system. Select an appropriate input probability distribution for each stochastic input variable and estimate corresponding parameters. Empirical

distributions are used when standard distributions are not appropriate or do not fit the available system data. Triangular, uniform or normal distribution is used as a first presumption when no data are available.

Step 4. *Formulate and develop a model.* Develop graphics and network diagrams of the system. Translate these *conceptual models* to acceptable form for the selected simulation software. Verify that the simulation model executes as intended. Verification techniques include traces, varying input parameters over their acceptable range and checking the output, substituting constants for variables and checking the plausibility of the results.

Step 5. *Validate the model.* Compare the model's performance under known conditions with the performance of the real system under the same conditions. Perform statistical inference tests and get the model examined by system experts. Assess the confidence that the end user places on the model and address eventual problems.

Step 6. *Document model for future use.* Record objectives and assumptions of the project as well as input variables and model's parameters in detail.

Step 7. *Select appropriate experimental design.* Choose a performance measure, a few number of input variables that are likely to influence it, and the levels of each input variable. When the number of possible configurations (product of the number of input variables and the levels of each input variable) is large and the simulation model is very complex, common second-order design classes including central composite or full-factorial should be considered. Document all details of the experimental design.

Step 8. *Establish experimental conditions for runs.* Address the question of obtaining accurate information and the most results from each run. Determine if the system's behaviour is stationary (performance measure does not change over time) or non-stationary (performance measure changes over time). Generally, in stationary systems, steady-state behaviour of the response variable is of interest. Select the run length. Select appropriate starting conditions and the length of the warm-up period (transient behaviour), if required. Decide the number of independent runs (each run uses a different random number string and the same starting conditions) by considering output data sample size. Sample size must be large enough (at least 3–5 runs for each configuration) to provide the required confidence in the performance measure estimates. Check if the output data is not correlated.

Step 9. *Perform simulation runs.* Runs were performed as specified in Step 8 above.

Step 10. *Interpret and present results.* Compute numerical estimates (e.g., mean, standard deviation, confidence intervals) of the desired performance measure for each configuration of interest. The assumption that batch means are independent may not always be true; increasing total sample size and increasing the batch length may be helpful. Test hypotheses about system performance. Construct graphical displays of the output data. Document results and conclusions.

Step 11. *Recommend further course of action.* This may include additional experiments to increase the precision and reduce the bias of estimators (e.g. to perform sensitivity analyses).

The most important stage in the preparation of the simulation project constitute the conceptual modelling. *Conceptual modelling* is the process of abstracting a

model from a real or proposed new system. The design of the model influences all aspects of the study, in particular the data requirements, the time in which the model can be developed, the validity range of the model, the speed of experimentation and the confidence and accuracy of experimentation results. Although effective conceptual modelling is a vital aspect of a simulation study, it is probably the most difficult and least understood (Robinson 2008). There are few publications to the subject of conceptual modelling. The main reason for this situation is due to the fact that conceptual modelling is more an ‘art’ than a ‘science’ and therefore it is difficult to define methods and procedures. The result is that the process of conceptual modelling is mostly learnt by experience. The main domain of interest for this chapter is the use of simulation for modelling of operating systems. Wild (2002) defined the term ‘an operating system’ as a configuration of resources combined for the provision of goods or services’. Wild identifies four specific functions of operations systems: manufacture, transport, supply and service. Models in these domains tend to be of a relatively small scale, with a project life-cycle of normally less than six months (Cochran et al. 1995). Simulation modelling in the military domain as well as for the global logistics networks tend to be of a much larger scale and where they are developed by teams of people.

Often the consequence of conceptual modelling is the need to formulate its concretisation in the form of a mathematical model. The mathematical model is characterized by the highest degree of abstraction and allows the use of universal symbols instead of specific physical quantities. We define *a mathematical model as a finite set of symbols and mathematical relations as well as strict operating rules, while the symbols and relations included in the model have an interpretation referring to specific elements of the modelled real system*. The set of symbols and relations is an abstract mapping of the system, and the factor transforming it into a mathematical model is a physical interpretation. *Mathematical modelling* is an interdisciplinary field whose task is to describe complex and sophisticated reality in the simplest possible and acceptable way. Thus, the only criterion for the correctness of modelling is the consistency of results obtained with its use with reality (generally identified with experience).

The process of a mathematical model building is characterized by an iterative procedure and it can be distinguished in the following five main stages (see Fig. 5.1): formulating modelling goals, selecting the model category and determining its structure, identifying model parameters, building a calculation algorithm, and verifying calculations results as well as validation of the model.

Stage 1. Formulating modelling goals

Models should be created for specific systems and phenomena, as well as applications, and therefore the modelling process must be targeted purposeful. Depending on the assumed modelling goal, we distinguish the following types of models:

- phenomenological models—whose function is to describe the operation of the system,

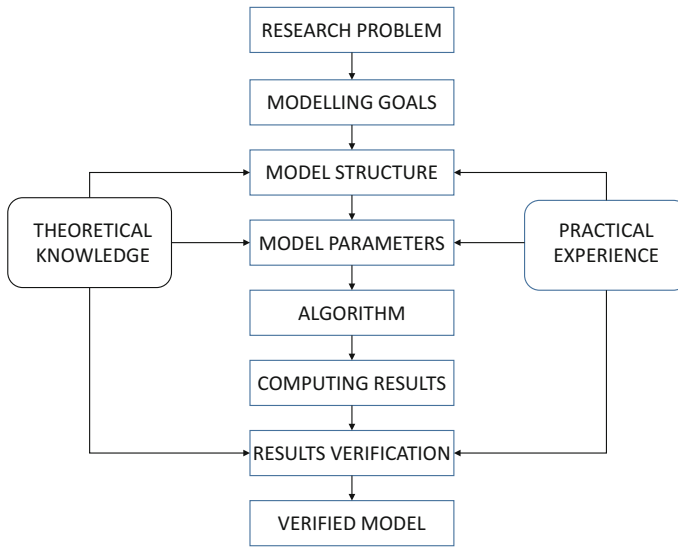


Fig. 5.1 The process of a mathematical model building

- prognostic models—which are used to predict system behaviour in the future under different environmental conditions,
- decision models—supporting the selection of inputs values, meeting certain conditions at the outputs of the system,
- normative models—supporting the selection of the structure and parameters of the system, fulfilling specific tasks.

Stage 2. Selecting the model category and determining its structure

The whole system-relevant knowledge about the system should be transformed into a set of consistent mathematical-logical relations. The most difficult in practice is to achieve a rational compromise between the degree of complexity of the model and the ease of its use (so-called degree of simplification). Another important problem related to the requirement of model's compliance with the modelled system is the significance problem. It consists in the proper distinction of the essential features of the modelled system, which must be reflected in the model. The difficulty usually consists in the lack of a priori appropriate theory and the need to verify it a posteriori using the results of modelling.

Stage 3. Identifying the model parameters

The identification of the model parameters means the estimation of the numerical values for coefficients occurring in the model. There are two possible ways:

- passive identification, consisting in collecting experimental data during the 'normal' operation of the system, and then determining the searched values of the model parameters with statistical methods (so-called estimation), or

- active identification, consisting in proper planning and conducting an experiment, the results of which will allow to determine the desired parameter values.

Active identification is used, for example, in cases where the ‘normal’ operation of the system takes place only in stationary conditions.

Stage 4. Building a calculation algorithm

Calculations in the application of mathematical models usually include solving of equations and inequalities using analytical, numerical and simulation methods.

- Analytical solutions lead to explicit results and allow the assessment of important system properties such as sensitivity and stability.
- Numerical solutions are used when the values of dependent variables can only be determined using appropriate algorithms. The solution algorithm is usually implemented by a computer program.
- Simulation solutions are characterized by the fact that the independent variables of the model correspond to the input quantities, and the dependent variables to the output of the real system. In the case of computer simulation, the numerical procedure is part of the simulation model.

Stage 5. Verifying calculations results and validation of the model

The model verification consists in comparing the results of modelling with the behaviour of the real system due to the compliance with the theoretical knowledge and the results of experimental research. The efficiency of model building can be increased by applying verification in all phases of model creation.

The compliance of the model with the system is validated according to the following criteria:

- internal, regarding the features of the model, such as formal compliance (i.e. no logical conflicts) and algorithmic compliance (i.e. the ability to perform calculations with the required accuracy),
- external, regarding the goals of modelling and compliance of modelled phenomena with theory and experimental data. The heuristic compliance refers to the scientific values of the model, such as the ability to interpret phenomena, verification of hypotheses, and the pragmatic consistency refers to the results of modelling, verified by comparing these results with the behaviour of the real system under the same conditions.

In general, situations in which simulation modelling and analysis is useful include the following cases:

- It is impossible or extremely expensive to observe certain processes in the real world.
- It is impossible or extremely expensive to validate the mathematical model describing the system (e.g., due to insufficient data).

- Problems in which mathematical model can be formulated but analytic solutions are either impossible or too complicated (e.g., complex systems like global supply networks).

Most simulation studies nowadays are implemented using a simulation software package. The main advantages are: reduced programming requirements, conceptual guidance, automated gathering of statistics, graphic symbolism for user friendly communication, visual animation, and possibility to change the model. Metrics for evaluation of this packages include: modelling flexibility, simplicity (ease for use), a variety of modelling structure (e.g. hierarchical, flat, object-oriented, network), code reusability, graphic user interface, hardware and software requirements, statistical capabilities, output reports, customer support, and documentation. The main types of simulation packages are simulation languages and application-oriented simulators. Admittedly, simulation languages offer more flexibility than the application-oriented simulators, but they require varying amounts of programming expertise. Application-oriented simulators are easier to learn and have modelling constructs closely related to the application.

The basic advantages of simulation techniques are (Maria 1997):

- Employ a systems approach to problem solving.
- Obtain a better understanding of the system by observing the system's operation in detail over any period of time.
- Test hypotheses about the system for feasibility.
- Compress time to observe slowly changing phenomena over long periods or expand time to observe a fast changing phenomenon in detail.
- Study the effects of different scenarios on the operation of a system by altering the system's model.
- Experiment with new situations about which only poor information is available.
- Identify the 'driving' variables (ones that performance measures are most sensitive to), and the inter-relationships among them.
- Identify bottlenecks in the flow of material, people, or information.
- Use numerous performance metrics for analysing system configurations.
- Develop well designed, reliable systems and reduce system development time.

However, simulation can be a time consuming and complex process with following pitfalls:

- Unclear objective.
- Erroneous assumptions.
- Invalid model.
- Simulation model too complex or too simple.
- Using the wrong input description.
- Replacing a random variable by deterministic value.
- Using the wrong performance measure.
- Not taking into account an initial bias in output data.
- Making only one simulation run for a configuration.
- Using simulation when an analytic solution is appropriate.

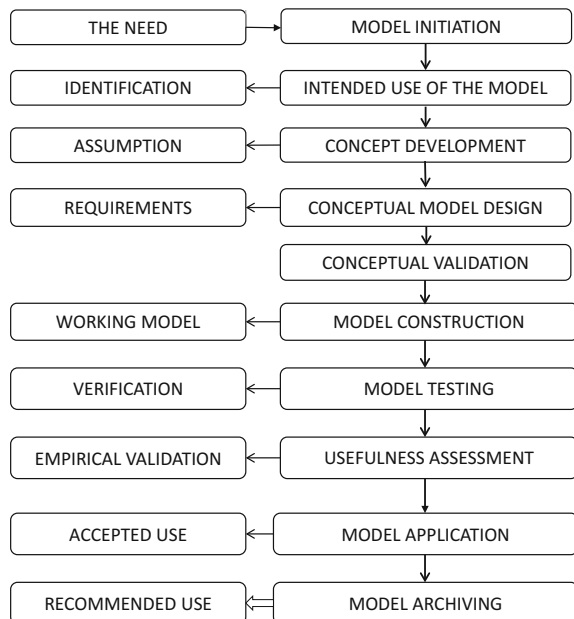
5.1.2 The Life Cycle of a Modelling and Simulation Process

The life cycle of a modelling and simulation (M&S) process has two main parts: M&S development, which includes initiation, concept development, design, construction, and testing; and M&S application, which contains application and archiving. These phases are shown as a general algorithm in Fig. 5.2.

The need for modelling and simulation starts their life cycle and can occur at any point in a program's or project's development. This need starts the M&S *initiation phase*, where the *real engineered system (RES)*, that needs to be modelled and simulated, and the information that are required are identified, as well as the intended use of the M&S is defined. The *intended use* is further defined during the *concept development phase*, where the aspects of the RES that need to be included in the M&S and the assumptions required to implement the M&S are identified. Next the objectives and level of detail required for the M&S, as well as acceptance criteria to determine M&S sufficiency, are identified. The intended use typically becomes more refined throughout M&S development, leading to iterations in the M&S development phase in case of the intended use changes.

During the M&S *design phase*, a conceptual model and other M&S requirements or specifications are developed to describe the physical behaviour of the RES and

Fig. 5.2 The life cycle of a modelling and simulation process



its interactions with the environment. This conceptual model is validated against the aspects and behaviour of the RES within the areas of interest as defined by the intended use during the conceptual validation phase. Once the conceptual model is validated, the *working model* is constructed. The relationships between the M&S design (conceptual model), the working model (computational model), and the RES (reality of interest) are illustrated in Fig. 5.3 (adapted from NASA 2016).

During the model *testing phase*, verification shows if the working model adequately represents the RES, and behaves similarly to real system. However, the intent of empirical validation is to identify the model's limits of operation, e.g. the area in which the model behaves correctly. When at the end of model testing the model is already verified and validated, the model's capabilities, assumptions, and limits of operation are documented and assessed with respect to acceptance criteria to determine the permissible uses of the model. Once model testing is successfully completed, the model is released, along with documentation of the model's capability and the range of the model applicability, ending the model development phase.

During the *application phase*, the use of a model starts with an assessment of whether or not the proposed usage of the model sufficiently matches the permissible ones. If the proposed use is acceptable, the model is then used to obtain the results of interest. If the proposed model does not meet the defined permissible use, the intended use will either be rejected or possibly allowed with the appropriate restrictions, caveats, or placarding required (NASA 2016).

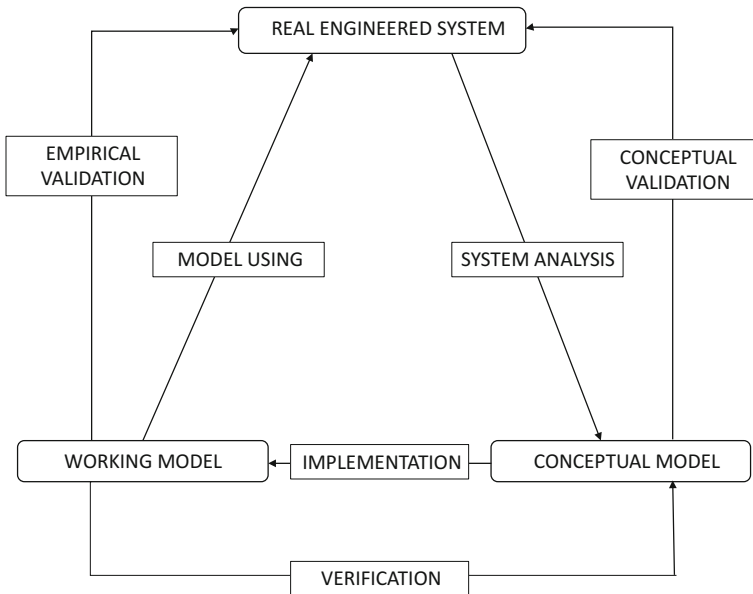


Fig. 5.3 The relationships between the conceptual model, the working model and the real engineered system (based on NASA 2016)

An important stage in the life cycle of a modelling and simulation process is the examination of M&S-based results credibility. The eight key factors contained in this assessment are considered as a minimum set and they are: data pedigree, verification, validation, input pedigree, uncertainty characterization, results robustness, M&S history, and M&S process/product management. These factors are grouped into three categories of M&S: Development (data pedigree, verification, validation), M&S Use (input pedigree, uncertainty characterization, results robustness) and Supporting Evidence (M&S history, M&S process/product management), which may span all aspects of an M&S Credibility Assessment Structure (NASA 2016).

The M&S Development category captures those aspects of the M&S that relate to the general purposes for which it was developed; the M&S Use (Operations) category addresses the aspects relevant to the current application of the M&S to generate the particular M&S results under assessment; and the Supporting Evidence category addresses two cross-cutting factors. The main aspects assessed by these eight factors include as follows:

I. M&S Development

- Data pedigree—in order to determine whether the pedigree and quality of the data used to develop the model is adequate and acceptable.
- Verification—allows to determine whether the models were implemented correctly, including their requirements and specifications.
- Validation—allows to determine whether the M&S results were close to the referent data and the reality of interest (RES).

II. M&S Operations

- Input pedigree—in order to determine whether the pedigree and quality of the data used to setup and run the model is adequate or acceptable.
- Uncertainty characterization—in order to determine whether the uncertainty in the current M&S results is appropriately characterized, as well as establish what are the sources of uncertainty are in the results and how they are propagated through to the results of the analysis.
- Results robustness—in order to determine how thoroughly are the sensitivities of the current M&S results known.

III. Supporting Evidence

- M&S History—allows to determine how similar is the current version of the M&S to previous versions, and how similar is the current use of the M&S to previous successful uses.
- M&S Management—allows to determine how well managed were the M&S processes and products.

Using a general-purpose software package for modelling and simulation, we should remember that some credibility assessment activities are two-fold: those relating to the package itself, and those relating to the implemented M&S process.

The former is usually given insufficient attention in the case of M&S using third-party tools, where certain aspects of M&S are neither performed nor managed for some aspects of M&S processes. Additionally, the particular computational model that is constructed using the tool is also evaluated in this category, which necessarily includes the pedigree of the data used in M&S development, as well as verification and validation of the constructed M&S. However, the M&S Operations category deals with the credibility factors for the application of the particular computational model in the generation of the current M&S results. This includes the present use of the model for the simulation, analysis, and reporting of the results. The use history of both the tool in general and the particular computational model, as well as the overall management of the M&S processes and products involved in the development, operation, and analysis of the computational model, are covered in the Supporting Evidence category (NASA 2016).

The decision about which cases of modelling and simulation should be subject to the rules outlined above depends on the result of the M&S risk assessment. Such risk assessments consider both the *consequences* to human safety or project success criteria if a decision proves incorrect, and the degree to which M&S results *influence* a decision.

Decision consequence classifications assess the impact of a decision that proves incorrect and include four different levels (based on NASA 2013):

- Class IV—Negligible. A poor decision may result in the need for minor ‘first aid’ treatment but would not adversely affect personal safety or health; damage to facilities, equipment, or hardware more than normal wear and tear level; cost overrun less than 2% of planned cost; all criteria met, with at worst minor performance degradations.
- Class III—Moderate. A poor decision may result in minor injury, or minor property damage to facilities, systems, equipment, or hardware; cost overrun between 2 and 15% of planned cost; moderate performance degradations.
- Class II—Critical. A wrong decision may result in severe injury, or major property damage to facilities, systems, equipment, or hardware; cost overrun between 15 and 50% of planned; substantial performance degradations.
- Class I—Catastrophic. A wrong decision may result in death or permanently disabling injury, facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission; cost overrun greater than 50% of planned cost; most criteria not met due to severe performance degradations.

Influence estimates the degree to which M&S results impact program or project engineering decisions. Engineering decisions include determination of whether design requirements have been verified and include five different levels (based on NASA 2013):

- Influence 1—Negligible. Results from the M&S are a negligible factor in engineering decisions. This includes research on M&S methods, and M&S used in research projects that have no direct bearing on program/project decisions.

- Influence 2—Minor. M&S results are only a minor factor in any program/project decisions. Test data for the real system in the real environment are available, and M&S results are used just as supplementary information.
- Influence 3—Moderate. M&S results are at most a moderate factor in any program/project decisions. Test data for the real system in the real environment are not available, but ample flight or test data for similar systems in similar environments are available.
- Influence 4—Significant. M&S results are a significant factor in some program/project decisions, but not the sole factor for any program/project decisions. Test data for similar systems in similar environments are available.
- Influence 5—Controlling. M&S results are the controlling factor in some program/project decisions. Test data are available for essential aspects of the system and/or the environment.

The results of the risk assessment should be presented in the form of a risk matrix, an example of which is shown in Fig. 5.4. Those M&S that are judged to fall within the red (R) boxes are obligatorily within the scope of the procedure described above, and those that fall within the green (G) boxes are not. The M&S that are judged to fall within the yellow (Y) boxes are recommended to be processed in accordance with the above procedure.

RESULTS INFLUENCE	5. CONTROLLING	G	Y	R	R
	4. SIGNIFICANT	G	Y	R	R
	3. MODERATE	G	Y	Y	R
	2. MINOR	G	G	Y	Y
	1. NEGLIGIBLE	G	G	G	G
		IV. NEGLIGIBLE	III. MARGINAL	II. CRITICAL	I. CATASTROPHIC
DECISION CONSEQUENCE					

Fig. 5.4 An example of a M&S risk assessment matrix (based on NASA 2013)

5.2 Modelling of Logistic Infrastructures—Agent Based Approach

5.2.1 *Fundamentals of Agent-Based Modelling and Simulation*

Agent-based modelling (ABM), is a computational framework for simulating dynamic processes that involve autonomous agents (agent-based simulation—ABS). An autonomous agent can act on its own without external direction in response to situations the agent encounters during the simulation process. Modelling a population of autonomous agents with its own characteristics and behaviours, which interact with each other and with the environment, is a main feature of an ABS. Agent-based simulation is most commonly used to model individual decision-making and social as well as organizational behaviour (Bonabeau 2001). Agents generally represent people, or groups of people, and their mutual relations represent processes of social interaction (Gilbert and Troitzsch 2005). In a supply chain, agents are firms which make decision about material sourcing and ordering, stocking, shipping, capacity expansion, etc. In an agent-based model composed of artificial agents, collaborating entities search the environment and communicate their findings to collectively accomplish a task. The development of agent-based modelling tools, the availability of data on agent transactions and interactions, and advances in computation have made possible a growing number of ABM and ABS applications across a variety of domains and disciplines.

A typical structure of an agent-based model has three types of elements: agents (their attributes and their behaviours), agent relationships and methods of interaction (an underlying topology of connectedness defines how and with whom agents interact), and agents' environment (agents exist in and interact with their environment).

I. Agents

In the context of agent-based modelling and simulation we consider that agents have following properties and attributes (Macal and North 2010):

- *Autonomy*—an agent is autonomous and self-directed. An agent can function independently in its environment and in its interactions with other agents, generally from a limited range of situations that are of interest and that arise in the model. An agent's behaviour refers to a general process that links the information the agent senses from its environment and interactions to its decisions and actions.
- *Modularity*—agents are modular or self-contained. An agent is an identifiable, discrete entity with a set of characteristics, behaviours, and decision-making capability. The modularity requirement implies that an agent has a boundary, and it is possible to determine whether something is a part of an agent or not.

- *Sociality*—an agent is ‘social’, interacting with other agents. Common agent interaction protocols include contention for space and collision avoidance, agent recognition, communication and information exchange, influence, and other application-specific mechanisms.
- *Conditionality*—an agent has a state that varies over time. Each agent has a state that represents the system condition, defined by the essential variables associated with its current situation. An agent’s state consists of a set or subset of its attributes and its behaviours. The state of an agent-based model is the collective state of all the agents along with the state of the environment. An agent’s behaviour is conditioned on its state.
- *Adaptability*—an agent may be adaptive, for example, by having rules or mechanisms that modify its behaviours. Agent behaviour modification can occur as a result of the learning process, e.g. based on its accumulated experiences. Individual learning and adaptation requires having memory as a dynamically updated attribute of the agent. At the system level, learning and adaptation can be modelled by aggregate changes in individual behaviours or by allowing agents to enter or leave the system, increasing the system effectiveness with the more successful agents.
- *Purposefulness*—an agent may have explicit goals that drive its behaviour, and criteria by which it can assess the effectiveness of its decision or action. This allows an agent to compare the outcome of its behaviours relative to its goals and adjust its responses and behaviours in future interactions.
- *Heterogeneity*—agents may be diverse. Unlike simple simulation that considers relatively homogeneous particles, agent simulations often consider the full range of agent diversity across a population. Agent characteristics and behaviours may vary in their extent and sophistication, they depend on how much information is considered in the agent’s decisions, the agent’s internal models of the external world, the agent’s view of the possible reactions of other agents in response to its actions, and the extent of memory of previous events the agent retains and can use in making its decisions. Agents may also be equipped with different amounts of resources or accumulate different types of resources as a result of agent interactions, further differentiating agents.

II. Agent relationships

The primary issues of modelling agent interactions are specifying who is, or should be, connected to whom, and describing the dynamics of the interactions. Common topologies for representing social agent interactions include (Macal and North 2014):

- ‘Soup’—a non-spatial model in which agents have no locational attribute,
- Grid or lattice—cellular automata represent agent interaction patterns and available local information by a grid or lattice. Cells immediately surrounding an agent are its neighbourhood. An agent’s location is the grid cell index.
- Euclidean space—agents roam in 2-dimensional or 3-dimensional spaces. An agent’s location is its relative or geospatial coordinates.

- Geographic Information System (GIS)—agents move over and interact with realistic patches of geo-spatial landscapes. An agent's location is a geographical unit (e.g., zip code) or geospatial coordinates.
- Networks—networks may be static (links pre-specified) or dynamic (links determined endogenously by relationship-creating mechanisms). An agent's location is the relative node location in the network.

The essential idea is that agents only interact at any given time with a limited number of other agents out of the population. This notion is implemented by defining a local neighbourhood (usually a network) and limiting interaction to a small number of agents that are in their neighbourhood. Agents do not have to be located in close proximity to one another spatially to be able to interact. The *network topology* allows agents to be linked on the basis of relationships in addition to proximity. Any agent may be a member of many different networks.

III. Agent environment

Agents interact actively with their environment and with other agents. The environment may be used to provide information on the spatial location of an agent relative to other agents or it may provide a full set of geographic information (e.g., as in a GIS). An agent's location, included as a dynamic attribute, is needed to track agents as they move across a landscape (e.g. traceability in supply networks), contend for space, acquire resources, and encounter other situations. Complex environmental models can be used to model the agents' environment. In some cases, the environment may be seen as a limitation to the agent's operation, and constrain agent actions. For example, the environment in an agent-based transportation model would include the infrastructure and capacities of the nodes and links of the road network. These capacities would create congestion effects (reduced travel speeds) and limit the number of agents moving through the transportation network at any given time.

IV. Emergence in agent-based models

One of the most important advantages of agent-based modelling is the possibility of presenting the phenomenon of emergence. Even simple agent-based models in which agents are completely described by deterministic rules and use only local information can self-organize and sustain themselves in ways that have not been explicitly programmed into the models. More complex models representing real-world phenomenon can also exhibit emergent behaviour resulting from agent interactions. Agent-based modelling algorithms based on emergence have led to specialized optimization techniques, such as ant colony optimization and particle swarm optimization, that have been used to solve practical problems (e.g., Bonabeau et al. 1999; Barbati et al. 2011).

V. Designing agent-based models

Identifying agents, accurately and precisely specifying their behaviours, as well as appropriately representing agent interactions are the keys for developing useful

agent models. The first step in the process of developing an agent-based model consists of identifying the agent types according to their attributes. Agents are generally the decision-makers in a system, whether they are human, organizational, or automated. As soon as the agents are defined, agent behaviours are specified. A normative model in which agents attempt to optimize a well-defined objective can be a useful starting point to developing more descriptive and domain-specific behavioural heuristics. Alternatively, we can begin with a bounded rationality model or a generic behavioural heuristic to describe agent behaviour, or a formal behavioural modelling framework such as the Belief-Desire-Intent (BDI) model (Wooldridge 2009). In addition to agents, an agent-based model consists of agent relationships. To define the agent relationships we need the methods that control which agents interact, when they interact, and how they interact.

Design is a key activity in building agent-based models. Modern software toolkits (e.g. based on an object-oriented approach) use a template design approach in which recurring elements are codified and reused for new applications. The Unified Modeling Language (UML) provides a set of tools in the form of diagrams for object-oriented software system design and representation that is independent of computer code implementation (Booch et al. 2005). An agent-based modeller refers to existing design patterns to model important features of a real-world system, such as how time should be treated in a model. Some agent-based models include a variety of advanced capabilities in their model such as: artificial intelligence and machine learning algorithms, geographical information systems (GIS), connections to relational databases, version control, and integrated development environments (IDEs).

Agent-based modelling can offer distinct advantages to conventional simulation approaches such as discrete event simulation (Law and Kelton 1991; Law 2007), system dynamics (Sterman 2000) and other quantitative modelling techniques. The agent-based modelling and simulation can be beneficial, if any of the following criteria are satisfied:

- The problem has a natural representation as being comprised of agents;
- There are decisions and behaviours that can be well-defined;
- Agents have behaviours that reflect how individuals (entities) actually behave;
- Agents adapt and change their behaviours;
- Agents learn and engage in dynamic strategic interactions;
- Agents have dynamic relationships with other agents, and agent relationships form, change, and decay;
- When it is important to model the processes in which agents form organizations, and adaptation and learning are important at the organization level;
- Agents have a spatial component to their behaviours and interactions;
- The structure of the system does not depend entirely on the past, and new dynamic mechanisms may be invoked or emerge that govern how the system will evolve in the future;

- When arbitrarily large numbers of agents, agent interactions and agent states is important;
- When process structural change needs to be an endogenous result of the model, rather than an input to the model.

5.2.2 Using Agent-Based Modelling and Simulation in Logistics

A typical supply chain consists of five stages: producers (P), distributors (D), wholesalers (W), retailers (R) who directly respond to clients’ demand, and customers (C) (Macal and North 2006). Multiple agents of different type exist at each stage creating a network of supply chain agents. Figure 5.5 shows an example of the simplified model of supply chain agents (nodes of the network) interconnected with lines (edges of the network). For simplicity, the following assumptions are made: we ignore suppliers, there is only one commodity, no transformation of goods is made, and no assembly of materials into products is required. The flows of goods and information in the form of orders between each stage as well as physical shipments are included in the model. The flows of payments and the complexities of pricing, negotiation, and financial accounting that this would entail are not included in this model but could be added. Periodic repetition of the work cycle consisting of the following four steps is assumed:

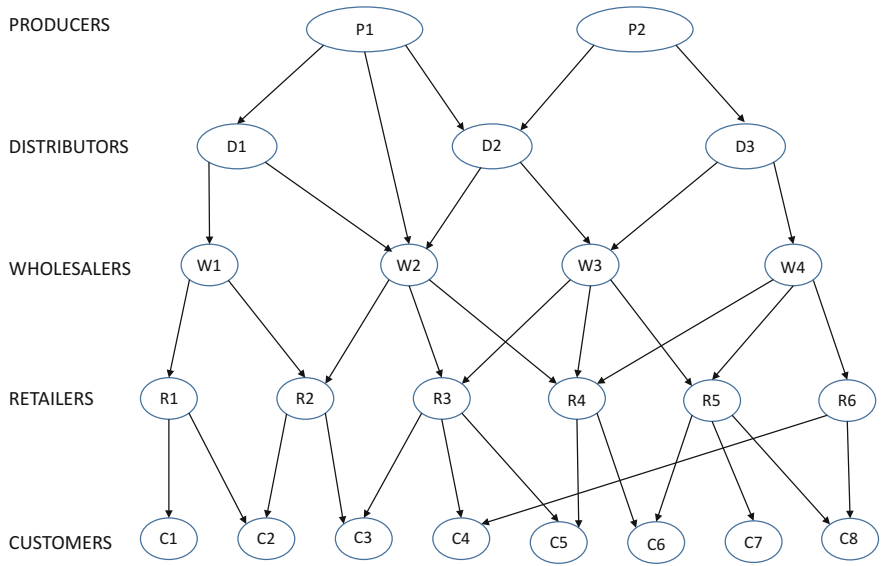


Fig. 5.5 The network of supply chain agents—an example

- (1) The customer places an order with the retailer.
- (2) The retailer fills the order immediately from its respective inventory in stock. If the stock does not have a sufficiently large number of ordered goods, the customer's order is placed on backorder and filled when stock is replenished.
- (3) The retailer receives a shipment from the upstream wholesaler in response to previous orders. He decides how much to order from the wholesaler based on an 'ordering rule', and estimates future customer demand using a 'demand forecasting rule'. The retailer then orders goods from the wholesaler to cover expected demand and any shortages relative to explicit inventory.
- (4) Similarly, each wholesaler receives a shipment from the upstream distributor, forecasts future demand by the downstream retailer, and places an order with the distributor. This process should be continued up the chain to the producer who decides on how much to put into new production.

The goal of the supply chain agents is to manage their inventory in such a way that minimizes costs through rational decisions based on how much to order each period (Swaminathan et al. 1998). When inventories are too low and there is a danger of running out of stock, agents increase orders; when inventories are too large and agents incur high inventory holding costs, agents decrease orders. Each agent strikes a balance between having too much inventory, which increase inventory holding costs, and too little inventory, which puts the agent at a risk of running out of stock and incurring excessive backorder charges. This example assumes that agents only have access to local information, thus no agent has a global view of the supply chain or is able to optimize the system as a whole. This simple agent-based model is a useful foundation for more realistic models of logistic networks in which the various simplifying assumptions have been relaxed and more complex agent decision rules are considered. Several agent models of supply chains have been developed with various enhancements such as agent access to global information and to modelling the endogenous development of agent relationships based on trust (Macal and North 2003; Macal 2004).

Starting from the above assumptions, we can begin building the agent-based simulation model by identifying the agent types and other objects along with their attributes—step 1. In this model, the supply chain agents consist of producer, distributor, wholesaler, retailer and customer agents. Everything in the model should be either an agent or an object; the objects include the clock and the set of output reports. The distributor, wholesaler, and retailer agents are grouped together in a class called 'middle-agents' because they all have the same structure in terms of their attributes and the methods. Each *agent class* is represented by a set of attributes and methods that operate on this agent class. For example, the producer agent is represented by the following attributes: the agent's name, inventory level, desired inventory level, amount in 'pipeline', desired amount in 'pipeline', the amounts (received, shipped, ordered, and demanded), various decision parameters, and the costs incurred of holding inventory or backorders. The values of these variables at any point in time constitute the *agent state*.

In step 2 we should specify the *environment* in which the agents exist and interact. For the supply chain model, the environment consists of external non-agent factors that influence agent behaviour. Next, in step 3, we have to specify the methods by which agent attributes are updated during the simulation in response to either agent-to-agent interactions or agent interactions with the environment. For example, in the supply chain model, the inventory level is an important attribute of each agent. Inventory is updated when orders and shipments are received and sent. These methods would be applied to the agents upon receipt of an order or shipment and affect the values of agent attributes. The producer class also has methods that more directly embody the agent's behavioural decision rules. These include a rule for determining how much to order and from whom at any point in time, embodied in the 'ordering rule' procedure, and a rule for forecasting demand, embodied in the 'demand forecasting rule' procedure.

In step 4 we have to add the methods that control which agents interact with whom, when they interact, and how they interact. We can develop a procedure for selecting which agents to interact with, based on a bidding process in which, for example, the least-costly producer agent is selected from among all producer agents by a distribution agent placing an order. The agent selection procedure could be appealed at every time period or when inventory levels reach specified thresholds (e.g. so-called safety level). The agent interaction procedure would consist of placing an order with the selected agent at the determined time. In addition to agents, the simulation model consists of agent relations. If agents are the nodes in the logistic network, agent relations are the links or edges in this network. It means that each agent relation involves two agents. For example, the producer-distributor relation includes the attributes of the number of good items in-transit from factory to distributor and the order in-transit from distributor to factory. Agent relations also have methods that operate on them just as agents have (e.g. get shipment, get order, get upstream agent, and get downstream agent).

The complete set of object class definitions and methods, parameter values, and initial values for all the agent and other object states constitutes a complete specification of an agent-based simulation model. We can implement such a model by either writing an object-oriented programme using programming languages (for example, the Java or C++), or using a higher-level agent-based toolkit such as AnyLogic (2018), NetLogo (2006), Swarm (Bonabeau et al. 1999; SWARM 2018) and many others. Any of these toolkits provides an extensive set of classes that encapsulate the basic functionality required by the agent models. For example, the functionality for the sequence of agent operations and interactions in the supply chain model and the control mechanisms that cause each of the agent methods to be invoked at the proper time or in the proper situation would be part of the functionality provided by the scheduler class of an agent-based software (Macal and North 2006).

5.3 Modelling of Logistic Processes—Dynamic Based Approach

5.3.1 *General Rules for Managing the Flow Processes*

Rational management of flow processes is a process that can be divided into four stages:

- Identification of processes in the organization,
- Modelling of basic processes,
- Implementation of model processes,
- Process monitoring and evaluation.

The *identification* of processes in the organization is aimed at identifying those processes that are necessary to achieve the organization's goals. This procedure can take place in two ways:

- 'Top-down' approach—means from top to bottom, starting from the company's strategy by defining the few key processes, to describing many support processes,
- 'Bottom-up' approach—means from bottom to top, starting from elementary actions (activities), by combining them into larger groups, up to individual processes and finally the macroprocesses.

Firstly the valuation of processes should be made (e.g. determining the weight of each process). The final effect of this stage is to determine: the type, number, content and structure of processes which are necessary to achieve the organization's objectives and meet the requirements of the clients.

The aim of process *modelling* is the qualitative evaluation and shaping (design or modification) of processes that are important to the organization, so that they ensure effective and efficient functioning of the organization. In process modelling, two main types of approach are used:

- Diagnostic—coming from the current state (how is it currently?), with an evolutionary nature (gradual improvement of existing processes) and
- Prognostic—going from the desired state (how should it be?), with an adaptive nature (designing the ideal, striving to achieve the model state).

By modelling a designed process the following rules should be followed:

- Extracting the process from its environment—each process must have its beginning and end.
- Process structuring—each process has its own internal structure and consists of elements.
- Determining the responsibility for the process—each process has its own 'owner'.

- Determining the subject of the process—each process performs some functions (production, service).
- Concentration on creating value—the components of the process which do not create added value should be eliminated.
- Shaping the course of the process—the best (due to the accepted criteria) configuration should be set for each process.
- Process input security—for each process it is necessary to ensure a reliable supply (e.g. materials, energy, information).

The *implementation* of processes consists in creating conditions for the efficient and effective introduction of a new or improved process and ensuring its proper functioning. The scope of activities in this area includes securing material resources (materials, equipment, premises, etc.), preparing the process owner and process teams to supervise and manage these processes.

The designed and implemented process should be continuously *monitored* and periodically *assessed*. This requires establishing:

- A collection of measurable parameters (attributes) that uniquely characterize a given process;
- The methodology of measurements (tools, methods and accuracy);
- Limit values for individual parameters and signalling methods in case of exceeding them (e.g. warning, alarm).

Control of monitoring results takes place in the following steps:

- Real-time (current) measurement;
- Determination of deviations from target values (e.g. required, normative);
- Assessment of deviation significance and analysis of its cause;
- Development of remedial activities to correct results and prevent deviations in the future.

The frequency of the control depends on the nature of the parameter. And so, for example:

- Process efficiency is measured and analysed at short intervals (e.g. hourly);
- The duration of the process, timeliness and quality—at longer intervals (e.g. weekly);
- Process costs—even longer intervals (e.g. monthly);
- Customer satisfaction—in the longest intervals (e.g. internal quarterly, and external half-yearly, or even annual).

5.3.2 *Classification of Processes and Their Properties—APQC Model*

Designing the organization infrastructure and processes refers to adjustment of its activities to internal structures and the changing environment. For this purpose, effective models should be applied, such as the Process Classification Framework (PCF)—the universal model developed by APQC (American Productivity and Quality Center). The model was created in 1997 and is under constant development, so that its database contains currently more than 8,500 descriptions of ‘good practices’ and comparative data that can be effectively used in benchmarking processes (APQC 2015).

The APQC Process Classification Model has four levels:

Level 1 includes twelve *process categories*, representing the highest level of generality of activities, divided into two groups:

Five categories of operating processes:

- 1.0—development of vision and strategy;
- 2.0—development and management of products and services;
- 3.0—marketing and sales of products and services;
- 4.0—delivering of products and services;
- 5.0—customer service management.

Seven categories of supporting processes (e.g. management and support services):

- 6.0—development and management of human capital;
- 7.0—information technology management;
- 8.0—management of financial resources;
- 9.0—acquisition, construction and management of property;
- 10.0—management of environmental protection and occupational health and safety;
- 11.0—management of external relations;
- 12.0—knowledge, improvement and change management.

Level 2 includes 62 process groups, covering smaller areas of activities carried out as part of operating processes (symbols 1.x to 5.x) and supporting processes (symbols 6.x to 12.x), e.g. process category 4.0—(delivering products and services) consists of the following groups of processes:

- 4.1—supply chain planning (planning and purchasing of necessary resources);
- 4.2—procure materials and services;
- 4.3—produce, manufacture and deliver product;
- 4.4—deliver service to customer;
- 4.5—management of logistics and warehousing.

Level 3 includes 265 processes, as the basic and main level of the model (symbols 1.x.y to 12.x.y), e.g. process group 4.2 (procure materials and services) consists of the following processes:

- 4.2.1—development of sourcing strategies;
- 4.2.2—selection of suppliers and development/maintain contracts;
- 4.2.3—ordering materials and services;
- 4.2.4—evaluation and development of suppliers.

Level 4 includes 797 activities (individual actions), described in detail within individual implementation processes (symbols 1.x.y.z up to 12.x.y.z), e.g. process 4.2.2 (selection of suppliers and development/maintain contracts) consists of the following activities:

- 4.2.2.1—selection of suppliers;
- 4.2.2.2—certification and validation of suppliers;
- 4.2.2.3—negotiation of contracts;
- 4.2.2.4—contract management.

5.3.3 *Process Specification Standards*

5.3.3.1 BPMN Notation—A Process Meta-model

BPMN (Business Process Model and Notation) language was developed in 2002 in the form of a single diagram (Business Process Diagram). In the current version, BPMN 2.0 is an extensive system that can be considered as a standard meta-model of processes (BPMN Tutorial 2018). This means that it is possible to transform models built in BPMN notation into ready-made computer programs, which is an important advantage in computerization of process management.

Three main types of the models built in BPMN 2.0 language can be distinguished, namely:

- demonstration models that show the general course of the process without details enabling a deeper analysis of the process,
- analytical models used for preliminary analysis of processes,
- executable models, containing an accurate description of the analysed processes, with all their significant elements clearly defined.

Components of BPMN notation are graphic symbols, which are divided into four main categories:

- flows objects describing the behaviour of the process, i.e.:
 - events—objects that map specific situations occurring in the process,
 - activities—tasks performed as part of the process implementation, which can be described by specific attributes,
 - gateways—objects connecting or separating process flows,
 - connecting elements—that enable the mapping of mutual relations between elements of the process,

- places of the process implementation—enabling inclusion of participants in the process,
- artifacts—that are not part of the process itself and are used to supplement the model with additional information.

An example of the use of BPMN notation is shown in Fig. 3.5 (Chap. 3).

5.3.3.2 EPC Notation—Event Chain Model

Modelling of event-driven processes enables EPC (Event-driven Process Chain) diagrams that can also illustrate flows in logistics processes. Graphic symbols of EPC diagrams allow to present process control structures in the form of a chain of events and functions (EPC 2018). Thanks to the template, e.g. Microsoft Office Visio EPC Diagram, the user can easily create a graphical model of any event-driven processes, including logistic processes.

The EPC diagrams use following blocks:

- Functions—basic blocks of a rectangular diagram. Each function corresponds to the performed activity,
- Events—presented in the form of rhombuses, occur before and/or after the function. Functions are combined using events,
- Connectors—events and activities are combined with them. There are three types of connectors, corresponding to the following logical operators: AND, OR and exclusive OR (XOR).

The EPC event chain model can be written as an ordered five:

$$EPC = (E, F, C, m, A) \quad (5.1)$$

where:

- E a non-empty set of events,
- F a non-empty set of functions,
- C a set of connectors,
- m a mapping that assigns the appropriate logical operator to each connector (e.g. AND, OR, XOR),
- A a set of arcs connecting the vertices E , F and C .

5.3.3.3 Flow Charts

Flow charts have been used for about 50 years in informatics (ideograms of J. von Neumann) and use symbolism for the presentation of process dependencies.

The most widespread techniques are:

- ANSI (American National Standards Institute),
- PERT (Program Evaluation Review Technique),
- CPM (Critical Path Method),
- HIPO (Input-Process-Output Hierarchy),
- Transaction flow diagrams.

Creating a flow diagram can be divided into the following stages:

- Process identification,
- Determining the beginning and end of the process,
- Distinction in the process of its constituent elements (partial processes and activities),
- Assigning appropriate graphic symbols to particular elements of the process,
- Drawing a graphic diagram,
- Diagram verification.

Symbols of the individual process elements according to the ANSI standard are available on the Internet, e.g. on the BreezeTree Software website (<http://www.breetree.com/article-exel-flowchart-shapes.htm>).

5.3.3.4 Entity Relationship Diagrams—ERD

Entity Relationship Diagram (ERD) is based on three basic categories (ERD 2018):

- Entity—an object as an element of the reality in which information can be stored. The object can be a living being (client, supplier, etc.), a thing (machine, material, product, etc.), an event (contract, forecast, order, etc.) and a place (department, warehouse, etc.)
- Relationship—a natural connection between two or more entities. They can be binary (between two entities, e.g. employee-warehouse) or multiple (between three, four or more entities),
- Attribute—a feature characterizing entities and relationships in a selective (keys), descriptive (verbal) and procedural (quantitative) manner. Attributes are divided into primary (basic features of a given entity or compound) and derivatives (determined on the basis of the values of other, usually primary, attributes).

Modelling processes using ERD takes place in four stages:

- Identification of entities—e.g. by means of SWOT analysis or heuristic methods,
- Development of a preliminary scheme of entity relationships—e.g. using situational analysis,

- Identification of attributes and relationships—e.g. by methods of analysing documents and files,
- Developing a full diagram of entity relationships—e.g. based on the rules of system operation and entity matrices.

The method based on entity relationships is structurally mature and is well suited to both analysis (auditing) and synthesis (design) of processes, especially information flows ones. In situations where the processes are complex and their mutual relations very complicated, using of ERD requires support by expert teams.

5.3.3.5 Data Flow Diagrams—DFD

The Data Flow Diagram (DFD) is a technique of analysis and design of processes based on a structural approach. It consists of a data flow graph, which describe the required functions of data processing, supplemented with a description of the activities carried out. Diagrams connect process functions to system objects, thus they are object-oriented. DFD modelling techniques are particularly often used as tools for the analysis and design of transaction systems and processes (DFD 2018).

DFD is based on four basic categories:

- Processes—functions transforming input data into output data,
- Data flows—movements from one system element to another,
- Depots—data storage for a specified period of time, in the form of homogeneous groups,
- External objects (so-called ‘terminators’)—objects belonging to systems that are not part of the analysed system (e.g. customer, supplier, bank, etc.)

The graphic presentation of the method is based on the modification of the symbolism used in graph theory. Process decomposition is usually executed hierarchically ‘top-down’, starting with a context diagram, and ending with the specification of that elementary functions which are not subject to further decomposition. The degree of process complexity translates into the number of intermediate levels representing the intermediate diagrams (e.g. complex processes are modelled at least on five hierarchical levels). Depending on the number of elements on each level of the hierarchy, DFD diagrams are symmetrical and oblique (asymmetrical).

The use of DFD diagrams is particularly useful in the case of processes that are accompanied by intense information flows, such as distribution logistics. Usually, the inductive thinking and a usage of the process approach dominate in the process of implementing the DFD method.

5.3.3.6 Petri's Network

Petri's network graph is an ordered triplet of the form:

$$N = (P, T, A) \quad (5.2)$$

where:

- P a non-empty set of places (nodes of the network),
- T a non-empty set of transitions,
- A a set of relations between places (arcs of the network).

The generalized Petri network is an ordered fifth of the form

$$NG = (P, T, A, W, M) \quad (5.3)$$

where:

- (P, T, A) the N network,
- W a function of arc weights, which assigns a natural number to each transition as a weight,
- M a function defined on the set of places called the initial marking of the N network. As a result of marking the network, its places are assigned non-negative integers called tags.

Places in the network represent passive system elements and can take certain states and collect certain objects (e.g. goods, information, clients, etc.). Transitions are active elements of the system and fulfil the role of transport or processing of objects. Relations represent the structure of the network, showing interconnections of individual network elements and directions of possible transitions. A graphic representation of the Petri network is the graph, in which the places P are represented in the form of circles, the transitions T of rectangles, and the relations A in the form of directed arcs. Marks in the form of dots are placed inside circles (places), which can be interpreted as the degree of load of a given place or fulfilment of certain conditions. If all entrance places to a given passage have a marker, then this transition is considered to be active and meets the conditions for the so-called 'rebuff'. As a result of each rebuff, the marking of the network changes, because the entry points to the rebuffed passage lose one marker and the starting points gain one marker.

Petri networks are an effective tool for modelling processes, allowing for conducting any structural analysis and testing of system dynamics with simulation methods. This is an important advantage of this method, especially in the case of the analysis of complex logistic networks characterized by significant variability (Arnold 1995). Figure 5.6 shows an example of using one of many Petri network modelling software available on the market.

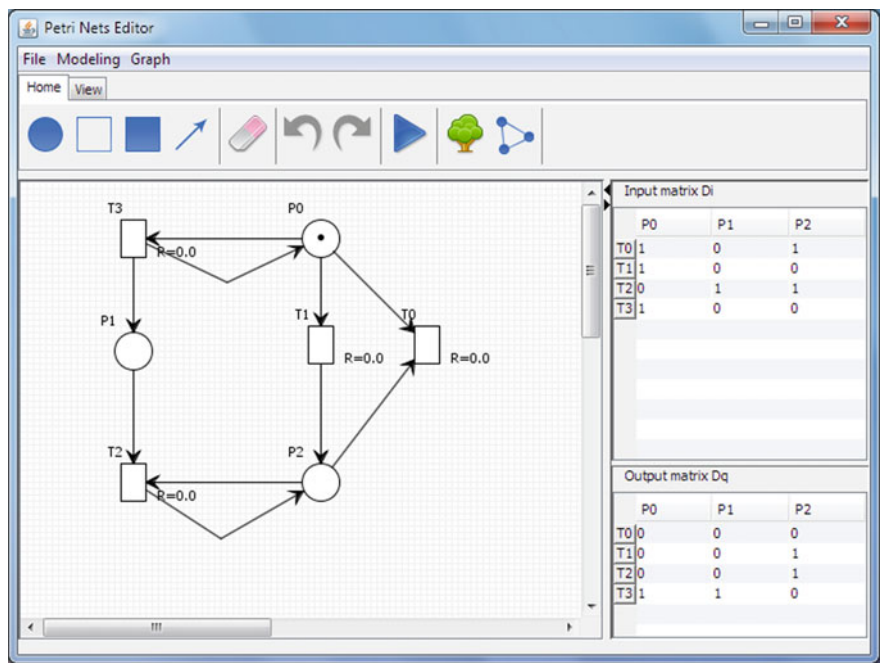


Fig. 5.6 An example of using the Petri nets editor to model a simple process (PETRI 2018)

5.3.3.7 Modelling of Value Flows—Value Stream Mapping (VSM) Method

Value Stream Mapping (VSM) is a technique that allows modelling the flow of values within any process (Seth and Gupta 2007). Thanks to this technique, we can exclude unnecessary activities in the process, and we can also adjust the process to the level of customer orders. The output parameter is a measure that results from the customer’s demand for products and determines the rate of implementation of the process subsequent stages. While mapping the value stream one should also take into account the frequency of material supply realized by suppliers, striving to minimize the inventory. The value stream map is a flow diagram of information and materials in the process. Value stream mapping consists of three stages:

- Stage 1. Value Stream Analysis (VSA)—making a diagnosis of the existing state based on the current value stream analysis.
- Stage 2. Value Stream Designing (VSD)—creating a vision of the future state by building the target status of the value stream.
- Stage 3. Value Stream Work Plan (VSP)—developing a plan for improvement and implementation of solutions.

The current state map presents:

- The state of the stream on a specific day of analysis;
- The state of the stream for the selected product, being a representative of a certain products family;
- Stream condition for average demand;
- Characteristics of key stream providers;
- Characteristics of key clients or groups of stream clients.

The purpose of the existing state map is:

- Presentation of the relationship between material and information flows;
- Identifying problems and waste in the stream;
- Determining the time used to process the components into a finished product expressed with L/T (*Lead Time*), and determination of the cash freezing period that was spent on components;
- Determining the time used to process components into a finished product expressed with P/T (*Processing Time*), that is, determining the possibility of shortening L/T for the stream, by streamlining the flow, eliminating stocks and waiting times;
- Creating the foundations for the construction of a state map for the future system configuration and an action plan.

The objectives of the mapping process are as follows:

- Build a system for managing the order fulfilment process;
- Define the principles of customer service, planning, supplying, inventory management and flow in the manufacturing process, enabling the execution of orders in the time required by the client and a form adapted to the value perceived by the client;
- Adapt the process to self-improvement and adaptation to a changing environment at the optimal costs;
- Create both short-term (e.g. 1 year) and long-term (several years) improvement plan;
- Build a production and logistics strategy.

In practice, a mapping procedure based on three pillars is recommended:

First, perceive the material and information flow, as well as inventories and process limitations;

Secondly, understand the transition time, customer needs, and other problems;

Thirdly, improve the whole value stream instead of local improvements.

An example of using the VSM method to describe a certain process is shown in Fig. 5.7.

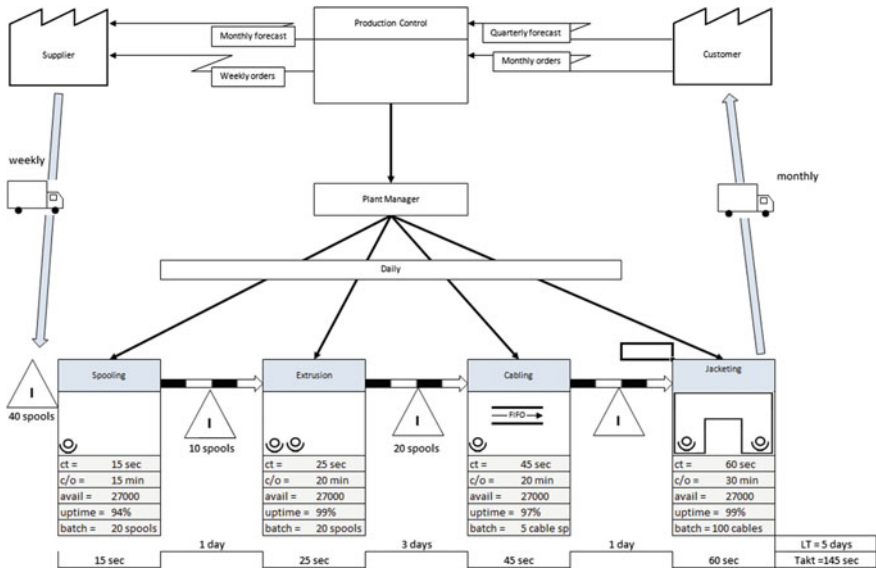


Fig. 5.7 An example of a process description using the value stream mapping method (...)

5.3.3.8 Reference Models—SCOR Model and Its Modifications

Reference models are sets of models (so-called process libraries) developed on the basis of experience gained over many years in various organizations. Many ERP systems offer such libraries for the main business processes (e.g. SAP R/3 library contains about 800 unified reference processes). Currently, the SCOR reference models are widely used in logistic practice

Reference Model SCOR (Supply Chain Operations Reference) was developed by the Supply Chain Council in 1996, and is still under development and modification (SCOR 2018). It is oriented on external processes of enterprises, and in particular supply chains. SCOR model is based on the concept of Business Process Reengineering, benchmarking and the best practice method.

The SCOR model includes, among others:

- Standard descriptions of management processes,
- Relationships between these processes,
- Metrics for process results,
- Management practices within the given industry,
- Standard configuration of functionality.

The SCOR model is built hierarchically, on three levels of detail:

Level I—defines the scope and content of the model in relation to four basic processes: planning ('plan'), supply ('source'), production ('make'), sales ('deliver') and returning ('return'), including their goals and measures (Fig. 5.8).

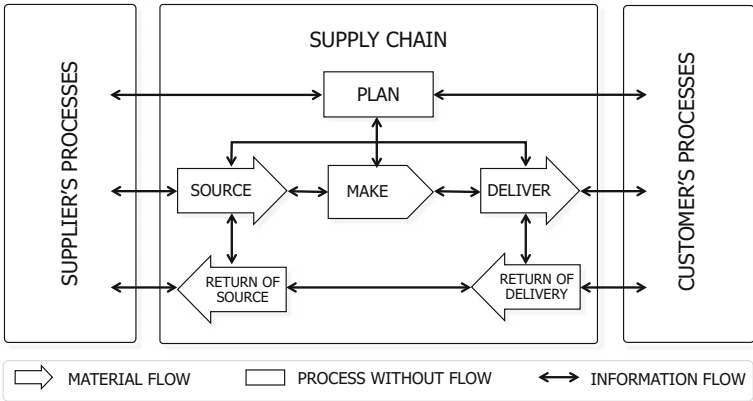


Fig. 5.8 Scheme of the process at level I according to the SCOR model

Level II—configures a supply chain composed of basic process categories.
Level III—decomposes the categories of level II processes into activities, including tasks, input and output data, and basic characteristics.

The assessment of the supply chain competitiveness using the SCOR model is carried out with the help of the so-called SCOR cards, which is a set of selected indicators allowing for a quantitative comparison of a given supply chain with the best in the industry. These indicators, describing the performance of the supply chain, are divided into two groups: customer-oriented and the company’s interior. The first group includes measures defining the reliability, reactivity and agility of the supply chain, while the second group includes costs and assets. An example of a supply chain performance attributes and level I metrics is shown in Table 5.1.

Table 5.1 Performance attributes and level I metrics

Performance attribute	Performance attribute definition	Level I metric (strategic)
Reliability	The ability to perform tasks as expected	Perfect order fulfilment (7R-rule)
Responsiveness	The speed at which a supply chain provides products to customers	Delivery time of the entire order cycle
Agility	The ability of supply chain to adapt to external changes	Upside SC flexibility Upside SC adaptability Downside SC adaptability
Costs	Operational costs of processes within the supply chain	SC management costs Cost of goods sold
Assets	The ability to use assets effectively	Cash-to-cash cycle time Return on SC fixed assets Return on working capital

An interesting modification of the SCOR model is the DCOR (Design Chain Operations Reference) model developed at the initiative of the Hewlett-Packard company, aimed at managing the design of supply chains. The model is based on five categories of processes, namely (Nyere 2008):

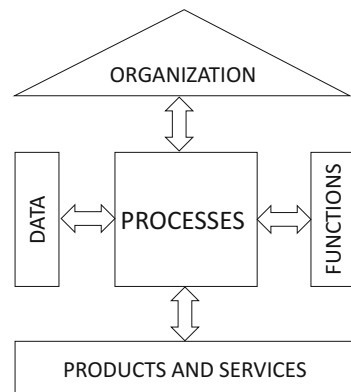
- Plan—focused on the selection of resources necessary to implement a specific supply chain in accordance with the requirements set for it;
- Research—consisting in the identification of tangible and intangible resources necessary to conduct research preceding the design of the supply chain;
- Design—creating a new solution or modifying an existing one, which does not meet the requirements set for it;
- Integrate—preparing the documentation necessary to provide operational support and marketing;
- Amend—suggesting changes based on a comparative analysis of the obtained effect in relation to the current status.

5.3.3.9 Reference Models—The ARIS Platform

The ARIS reference model is based on the concept of A.W. Scheer from 1991 (Architecture of Integrated Information System) and later House of Business Engineering. It uses the method of event control processes for modelling. SAP AG chose the ARIS system as a framework and methodical tool for the R/3 class reference models. This model is oriented towards internal processes of a production or service organization (ARIS 2018).

The concept of process modelling in the ARIS platform is based on five perspectives that create the so-called ‘ARIS house’ (Fig. 5.9). The basis of the home is the perspective of products and services, which captures static relations between material and non-material resources being inputs and outputs of processes. At the level of the ‘first floor’ there is data describing the state and the functions in a given organization. The ‘roof’ level represents the perspective of the entire organization,

Fig. 5.9 ARIS house—modelling perspectives and their mutual relations



while all these perspectives are directly connected with the perspective of processes that unites particular perspectives into one coherent whole.

The tools used by the ARIS platform have been divided into four classes (Scheer et al. 2006):

- ARIS Strategy Platform—is a module designed to define, implement and control the status of the organization's strategy;
- ARIS Design Platform—is a module for modelling, simulation and optimization of processes as well as IT architecture management in the organization;
- ARIS Implementation Platform—is an environment used to transfer process models to the level of IT applications, e.g. to the SAP system, creation of SOA structures (Service Oriented Architecture) and business rules management;
- ARIS Controlling Platform—is a module designed to monitor the dynamics of changes occurring in the organization, implementation of corporate governance systems, risk management and compliance with legal regulations.

In addition, the ARIS platform is equipped with the Business Optimizer tool, allowing to visualize the processes taking place in the organization and to carry out ongoing analyses of effectiveness and controlling. An example of using the ARIS platform for modelling logistic processes is shown in Fig. 5.10 (https://www.google.pl/search?q=aris+examples&biw=1644&bih=906&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwicy_na3qvKAhWDiwhKHZg2CMYQsAQIGg#imgrc=6P2Wp74zIy_iRM%3A).

Modelling business processes using the ARIS platform is simple and effective. Thanks to the 'top-down' approach, it allows for logical and clear presentation of all processes important for the organization and their optimization, but with a strong emphasis on the company's internal processes, not supply chains.

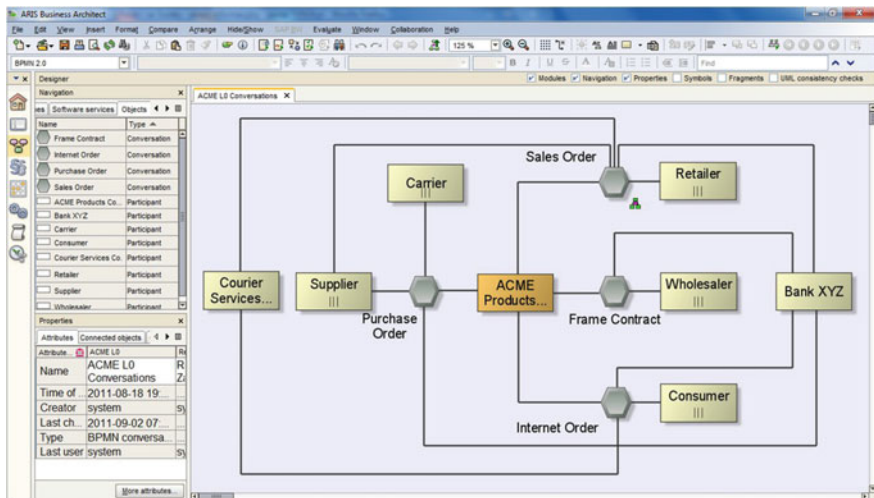


Fig. 5.10 An example of using the ARIS platform for modelling logistic processes

5.3.4 *Process Dynamic Modelling and Simulation*

Two methods are mainly used to model the dynamics of processes, namely: System Dynamics Modelling (SDM) and Discrete Event Simulation (DES). SDM offers a methodology to support the analysis of dynamic processes. A SDM model captures the factors affecting the behaviour of the whole system under consideration in a causal-loop diagram. This diagram clearly depicts the linkages and feedback loops among the individual elements in the system, as well as all pertinent linkages between the system and its operating environment. This type of analysis can be especially valuable to a decision-maker in understanding a complex engineered system by creating opportunities to model a variety of scenarios and observe how the system might perform under different conditions (Sweetser 2009).

System Dynamics (SD) is a computer-aided approach for analysing and solving complex problems with a focus on policy analysis and design. The field developed by Jay W. Forrester at the Massachusetts Institute of Technology, was initially called Industrial Dynamics (Forrester 1958). System Dynamics has its origins in control engineering and management; the approach uses a perspective based on information feedback and delays to understand the dynamic behaviour of complex physical, biological, and social systems. Forrester (1961) defines Industrial Dynamics as “... the study of the information-feedback characteristics of industrial activity to show how organizational structure, amplification (in policies), and time delays (in decision and actions) interact to influence the success of the enterprise. It treats the interactions between the flows of information, money, orders, materials, personnel, and capital equipment in a company, an industry, or a national economy”.

System Dynamics is well suited to modelling continuous processes, systems where behaviour changes in a non-linear fashion, and systems where extensive feedback occurs within the system. SD models often incorporate qualitative aspects of behaviour that might significantly affect the performance of a system. Its causal loop diagrams are an effective way of depicting feedback and linkages within a system. However, animation associated with a running SDM simulation model is usually limited to updating graphs and numerical displays (Morecroft 2015).

In SDM concept, the components and relationships among the components of a system build the structure of the system which determines its performance. Based on the proper defining of the linkages between people, organizations, processes, and resources, the structure of a system can be optimized to improve performance. These links are modelled by feedback loops, where a change in one variable affects other variables in the system, which makes SDM models ‘dynamic’. Another key concept in system dynamics is the ‘mental model’. These mental models can be characterized as flexible, rich in information, and able to integrate data from diverse sources. A significant part of the SDM effort is therefore associated with capturing these mental models using a causal loop diagram that represents the system’s behaviour.

SDM describes the behaviour of systems using differential equations. Because of the nature of these mathematical functions, SDM is well suited to modelling continuous systems. However, SDM is less well suited to providing a detailed representation of a

system with discrete changes in state variables, or mixed systems of both discrete and continuous processes (e.g. inter-arrival rates of discrete entities in a system).

The application of SDM to Logistics (e.g. in area of Supply Chain Management) has its roots in the fundamental works of Forrester (1958, 1961). His model of a production-distribution system is described in terms of 6 interacting flow systems, namely: the flows of information, materials, orders, money, manpower, and capital equipment. Based on the development and use of a System Dynamics simulation model, Forrester describes, analyses, and explains issues evolving around supply chain management (Angerhofer and Angelides 2000).

Based on Forrester's SD model Sterman (1989) developed a generic model of a stock management system, which forms the basic structure in an environment for a decision-making process. This generic stock management model can be applicable to many different scenarios, including raw material ordering, production control, or at a macroeconomic level, the control of the stock level and costs. The model consists of two parts: the physical stock and flow structure of a given system, as well as the decision rules used to control the system.

He stated that "in most realistic stock management situations the complexity of the feedbacks among the variables precludes the determination of the optimal strategy" (Sterman 1989), and proposed an order decision model based on a locally rational heuristics. An anchoring and adjustment policy is characterised by a mental simulation process, where an unknown quantity is estimated through recalling a well-known reference point (called the anchor), and then adjusting it according to other factors. Sterman (2001) suggested that the decision-making process is dominated by locally rational heuristics, due to the complexity of the system and time pressure, under which decisions are taken. Further factors to be included in this hypothesis of decision-making are: the availability, timeliness and perceived accuracy of information regarding the supply line.

Figure 5.11 shows the model of a simple supply chain system built using the iThink software that captures the flow of product across three sectors: production, distribution and *retail*. The production decisions are based on the demand from the retail sector and the company's current stock holding position. The production rate depletes the stock of raw materials. Finished goods are shipped based upon retail demand and flow down multiple distribution channels where they become part of the retailer's stock holding. The retailer sells goods to the end user and places orders based upon retail demand and the current levels of stock relative to the target level of stock (<http://www.properformasimulation.co.uk/technology.html>).

We will use the term Discrete Event Simulation (DES) for the modelling approach based on the concept of entities, resources and block charts describing entity flow and resource sharing (Cassandras and Lafortune 2009; Fishman 2001). This approach roots to 1960s when Geoffrey Gordon conceived and evolved the idea for GPSS and brought about its IBM implementations (Gordon 1961). Entities (or transactions in GPSS) are passive objects that represent people, parts, documents, tasks, messages, etc. They flow through the blocks of the flowchart where they wait in queues, are delayed, processed, split, combined, etc. (Borshchev and Filippov 2004). The AnyLogic view of the discrete event flowchart is shown in

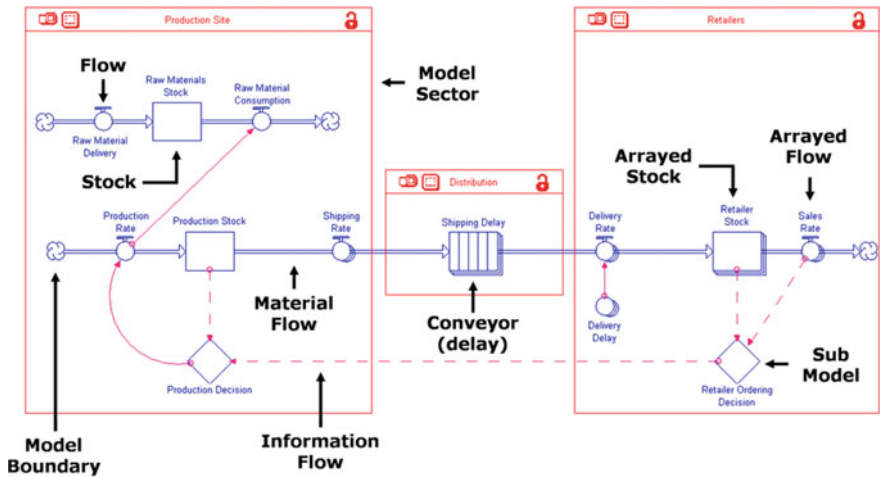


Fig. 5.11 An example of a stock management system modelling using the iThink software (<http://www.properformasimulation.co.uk/technology.html>)

Fig. 5.12 (https://en.wikibooks.org/wiki/Simulation_with_AnyLogic/Discrete_Event_Simulation/Ophthalmology_Department_Model/Step_5_Creating_a_flowchart).

A properly built DES model can replicate the performance of an existing system very closely and provide a decision-maker insights into how that system might perform if modified, or how a completely new system might perform. To achieve a

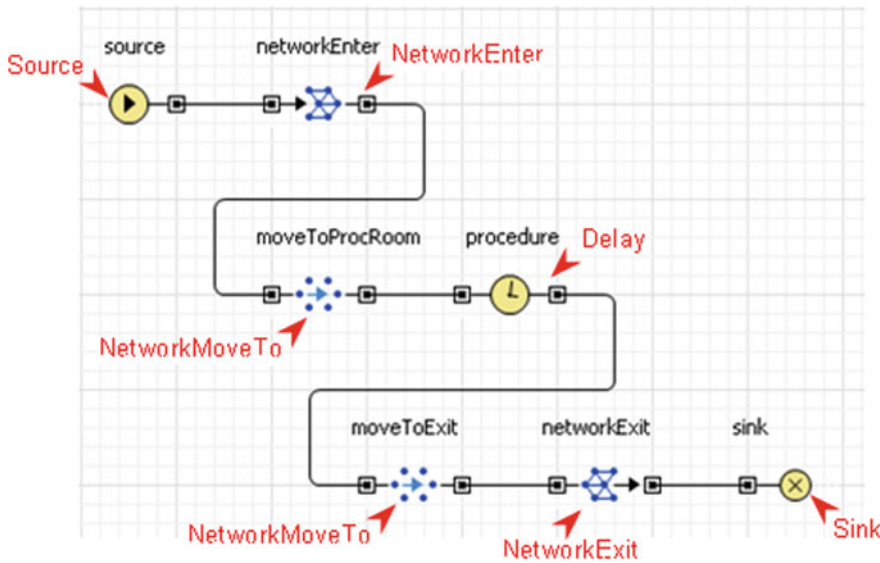


Fig. 5.12 An example of the discrete event flowchart created in AnyLogic

satisfactory fidelity to the performance of a real process, a DES model requires accurate data on how the system operated in the past, or accurate estimates on the operating characteristics of a proposed system. Like SDM, DES also gives the decision-maker the capability to model and compare the performance of systems and processes over a range of alternatives. DES is more appropriate to the detailed analysis of a specific, well-defined system or linear process, such as a manufacturing line or a service centre. These systems change at specific points in time: resources fail, operators take breaks, shifts change, or damage occurs. DES can provide statistically valid estimates of performance measures associated with these systems or processes, such as number of entities waiting in a particular queue or the longest waiting time for service.

Most software based on discrete event simulations concept (DES) include graphs and numerical displays, as well as a computer animation of the system. In these animations, icons represent entities moving through a graphical representation of the system. The process flow visualisation in a DES-animation can be a valuable tool to improve understanding of a process. DES, “concerns the modelling of a system as it evolves over time by a representation in which the state variables change instantaneously at separate points in time.” (Law and Kelton 1991). Therefore, it is used to gain an understanding of how an existing system behaves, and how it might behave if changes are made in the system.

Instead of a causal loop diagram (as in SDM), DES models are often built based on a process map, or a flow chart. These process maps can also support the clarifying of important processes and relationships. The important difference between SDM and DES is that SDM more often models abstract, general systems, such as a complex engineered system (e.g. SoS). DES models, in contrast, typically have a narrower focus. In these instances, process maps are just as important, but the systems under study tend to be easier to define. DES models more often reflect systems where entities are processed in a linear manner. Feedbacks play less of a role in these systems, whereas, it plays a large role analysing historical data to capture process parameters means, variances, and distributions. There is less emphasis in DES models on identifying events that might trigger changes in the model’s parameters (e.g. risk sources). Feedback loops can be built into discrete event simulations, however, their presence is less common than in SD models. DES models are often used when the main goal is a statistically valid estimate of system performance. There is a large area of overlap between the two approaches. Many problems could be modelled with either approach and produce results that would look very similar. Both methods, used appropriately, can help provide increased understanding and serve as an aid to decision-making. In many cases, the combination of both of these methods in one unit can be the best solution. Some examples of application of the above described modelling and simulation methods are included in the works (Bukowski and Karkula 2003, 2009, 2010).

5.4 Modelling of Demand Variation in Logistic Networks—Probabilistic Approach

5.4.1 Predictable Volatility

In situations where the variability of the environment is the nature of random fluctuations the use of statistical methods and time series is fully justified. These methods are well known, and their implementation is relatively simple (thanks to existing packages of computer software such as e.g. Excel, or more complex and sophisticated like Statistica, etc.). Basic statistical, probabilistic and time series models, which can be used effectively to describe the variability of the logistics network environment, will be briefly discussed below.

5.4.1.1 Statistical Methods

Mathematical statistics include description and analysis of repetitive phenomena using the assumptions of probability theory. Descriptive statistics, most commonly used in statistical analyses, allows to develop the results of a random sample without using the probability calculation methods. Statistical methods allow to draw quantitative conclusions about a general population, understood as a set of elements $\{E\}$ subject to research due to one or more features (e.g. X), based on studies of so-called random sample. The n -element random sample is a finite subset of elements of the general population, drawn in such a way that each subset consisting of n elements of the general population has the same chance of being drawn (Bukowski1995).

In order to conduct statistical analysis we should take the following steps:

- clearly define the general population $\{E\}$,
- take an n -element random sample from it— $\{e_1, e_2, e_3, \dots, e_n\}$,
- define the examined feature of the general population X ,
- determine the values of the X feature for each element of the random sample— $\{x_1, x_2, x_3, \dots, x_n\}$.

For such a set of numerical values $\{x_1, x_2, x_3, \dots, x_n\}$ we determine the basic statistical parameters, which are estimators of the central tendency, dispersion and frequency distribution of the examined feature X for the whole general population.

The most commonly used measures of *central tendency* are:

- arithmetic average

$$x_m = \frac{\sum_{i=1}^n x_i}{n} \quad (5.4)$$

- geometric mean

$$x_G = \sqrt[n]{x_1 x_2 \cdot \cdot x_n} \quad (5.5)$$

- median value—when n is an odd number the central number in an orderly, non-descending sample; and when n is an even number the arithmetic average of the two middle numbers.
- modal value (dominant)—the most frequently repeated, greater than the smallest and the smallest value.

The most commonly used measures of *dispersion* are:

- Range

$$R = x_{max} - x_{min} \quad (5.6)$$

- Interquartile range (IQR)—the difference between the upper and lower quartiles, contains 50% of the total number of the set, where:
 - the p -th percentile in the n -ordered set of numbers (e.g., random sample) is the value below which $p\%$ of the numbers of this set are located,
 - lower quartile—25th percentile,
 - upper quartile—75th percentile.
- Variance (arithmetic mean of squared deviations from the mean value)

$$V = \frac{\sum_{i=1}^n (x_i - x_m)^2}{n - 1} \quad (5.7)$$

- Standard deviation

$$s = \sqrt{V} \quad (5.8)$$

- Coefficient of variation

$$v = \frac{s}{x_m} \quad (5.9)$$

Typical *frequency distribution*—histogram

In the case of a small random sample size (up to 20), the data is sorted in a non-decreasing series and graphically represented in the coordinate system (X, N), where $X = \{x_1, x_2, x_3, \dots, x_n\}$ —elements of the series, while $N = \{n_1, n_2, n_3, \dots, n_m\}$ —frequency of individual elements of the series. If the values in the random sample are not repeated, then $m = n$.

In the case of a larger random sample size (over 20), the sample values are grouped in classes, i.e. in intervals (usually the same length), with a size of 5 to 20. The procedure takes place in the following steps:

- The number of classes is taken from an approximate formula

$$k \cong \sqrt{n} \quad (5.10)$$

- Absolute frequency— n_i , it is the number of results in a given class
- Relative frequency

$$r_i = \frac{n_i}{n} \quad (5.11)$$

- Accumulated frequency (absolute or relative)—the sum of the frequency values from the beginning of the distribution series to a given class.
- Distribution series—a series created from pairs of numbers representing the means of successive classes and their numbers.
- Histogram—distribution series presented in graphic form.
- Frequency polygon (broken frequency)—curve obtained by combining the means of successive classes on the graph in the form of a histogram.

5.4.1.2 Time Series Methods

Time series is a set of feature values in chronologically ordered, different moments (intervals) of time. Statistical analysis of time series is aimed at detecting the regularity to which the phenomenon under study is subject and is the basis for forecasting the course of this phenomenon in the future. It is assumed that the observed time series is one of many possible realizations of a discrete stochastic process, and that the stochastic process is stationary (at least in a broader sense) as well as ergodic. The stationarity assumption ensures immutability in time, while the assumption about ergodicity allows to accept that the values of a stochastic process distant in time are mutually uncorrelated or very poorly correlated (Woodward et al. 2012).

For prognostic purposes, it can be assumed that the stochastic process is a resultant of a certain deterministic process related to the impact of the so-called main causes, and a random process related to the so-called side causes. Based on this assumption, two components can be distinguished in the analysed time series:

- a systematic component related to the deterministic process and
- a random component, also called a random variations, related to the stochastic process.

The systematic component may occur in the form of: a trend, a fixed level of a forecast variable or a periodic component, which may be cyclical or seasonal. The trend is a long-term propensity for one-way changes (increase or decrease) in the value of the variable under investigation. It is a consequence of the certain factors operation on the forecasted phenomenon. Constant level means no trend and oscillating the value of the variable under study around a certain constant level,

corresponding to the average value. Cyclic fluctuations are long-term fluctuations in the value of the variable under study around the trend or fixed variable level. Seasonal fluctuations are changes in the value of the projected variable around the trend or constant average level of the variable, repeated every certain period (approximately constant), not exceeding one year.

The process of extracting individual components of the time series is called the decomposition of the time series, and it is carried out by building models of the time series. Depending on the assumptions made about the influence of particular components, their mutual relations and the method of determining parameters, these models may have a different form. There are three basic groups of models, in relation to which different tools for building prognostic models are selected depending on the structure of the time series:

- a. time series models with a constant level of the forecasted variable,
- b. time series models with the trend,
- c. time series models with a periodic component.

a. *Time series models with a constant level of the forecasted variable*

The modelling tools used in this group are relatively simple, and the accuracy of the forecast depends on the internal variability of the time series. Internal variability can be estimated using coefficient of variation (see Formula 5.7).

The following methods can be used in this class of time series:

- naive method,
- ordinary moving average method,
- weighted average moving method,
- exponential smoothing method.

b. *Time series models with a trend*

In the case where the time series consists only of the trend and random variations we can use one of two approaches: passive or active approach. If the developmental trend is constant and does not change over time, then the passive approach is applied based on analytical methods of trend forecasting. Analytical methods of isolating the trend are based on linear, exponential, polynomial or logarithmic functions.

In the case that the development trend can change over time, it is recommended to use active methods, for example Holt linear models. Active methods are based on the smoothing of time series which have both a developmental tendency and random variations occurring over time. These are exponential smoothing models described in two equations—the first of them is the model of the averaged time series, and the second is the average trend.

c. *Models of time series with periodic components*

These models are particularly well suited to forecasting changes in demand for many products and logistics services. Many goods and services are subject to the

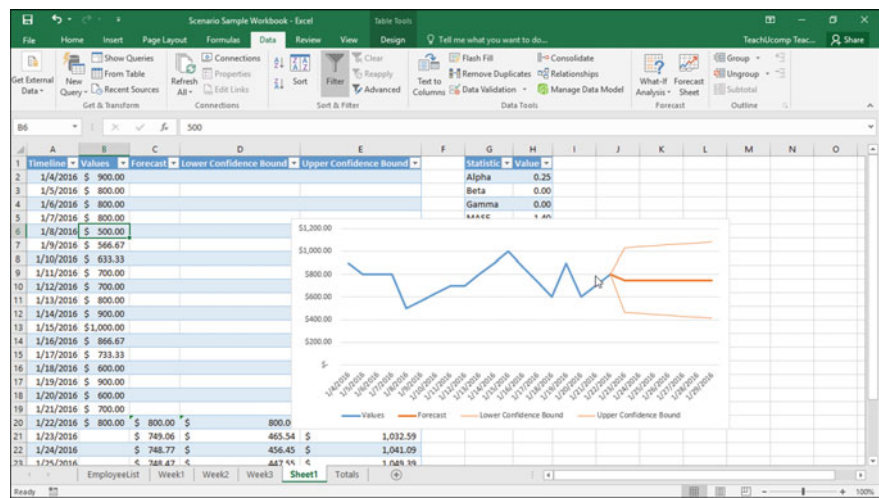


Fig. 5.13 Modelling time series with the excel forecast sheets to predict future trends from existing time-based data—an example (<https://www.teachucomp.com/forecast-sheets-in-excel-2016-tutorial/>)

so-called seasonality, so in forecasting models regarding demand for them one should take into account both the trend and the character of periodicity. In the case of series with the seasonal component, two basic methods are used: seasonal decomposition and the Winters model.

Most of these models can be successfully programmed in Excel (an example is shown in Fig. 5.13).

5.4.2 Unpredictable Variability

In cases where there is not enough information to use statistical or time series methods, there is a need to use inaccurate methods, based on analogies and expert intuition. We include analogue and heuristic methods. Below, both these groups of methods will be discussed in more detail, in particular in the aspect of the applying possibility to forecasting events and processes occurring very rarely, and which may have a big impact on the functioning of logistics networks.

5.4.2.1 Modelling by Analogies

These methods are used to predict the future behaviour of a variable (discrete—i.e., an event, or continuous—i.e., process features) based on data about similar variables, for which there is not enough evidence for causal relationships with the

researched variable. There are four basic types of methods, depending on the type of analogy underlying the inference and forecasting:

- methods of biological analogies, consisting in transferring the construction and functioning of living organisms to other objects, e.g. the structure of the system behaving in a similar way to animated organisms,
- spatial analogy method, consisting in predicting the occurrence of a specific event based on information about the occurrence of such an event in other territories, e.g. the appearance of certain events in one country allows us to assume that they will also appear in other countries,
- a method of historical analogies, consisting in transferring the regularity of changes in the time of one phenomenon to other phenomena occurring in the same object, e.g. the development of a certain type of logistic services may be the basis for predicting development trends of other new generation services,
- spatial-temporal analogy method, consisting in transferring regularities of changes over time from one object to other. In these methods there are usually identical variables, e.g. the tendency to increase the use of smart logistics tools in highly developed countries will also occur later in less developed countries.

The first two types of methods are generally qualitative, while the other two are also suitable for quantitative description.

The basic criteria for determining the similarity of variables are:

- the level similarity criterion, according to which two variables are similar if at a given moment or period they have reached a similar value - this criterion can be used only in relation to the fully identifiable variables;
- shape similarity criterion, according to which two variables are similar if they are characterized by similar character of changes in time - this criterion can be applied to each type of variables.

The usefulness of predictions determined by means of analogy is assessed with the help of opinions of independent experts, and the final criterion of the quality of the method is the value of 'ex post' errors, estimated after the expiry of the forecast.

5.4.2.2 Heuristic Methods

Heuristics generally means the ability to detect new facts and find connections between facts, especially using hypotheses. On the basis of existing knowledge, hypotheses are put forward that do not have to be proven. In computer science, heuristics is a method of finding solutions for which there is no guarantee to find the optimal solution, and often even the correct one. These solutions are used, for example, when the full algorithm is too expensive for technical reasons or when it is unknown (e.g. by long-term predicting the weather or by detecting certain unexpected hazards). This method is also often used to find approximate solutions, on

the basis of which, if possible, the final result is calculated using a full algorithm (Albar and Jetter 2009; Gigerenzer and Gaissmaier 2011).

The basic features of heuristic methods can be presented in the following way:

- they are models of phenomena existing in reality,
- they have a non-deterministic nature,
- they represent a parallel, simultaneous approach (e.g. multi-agent models),
- they have adaptive abilities that enable modification of models and their parameters.

Such types of features have methods included in the so-called *computational intelligence*, such as: genetic and evolutionary algorithms, artificial neural networks, ant algorithms, multi-agent systems, etc. (Karkula and Bukowski 2012). These methods have both many theoretical studies and practical applications, so they will not be discussed in this work.

Heuristic methods are based on an expert knowledge. At least several experts should participate in the creative process, and when selecting them the following aspects should be taken into account:

- the expert group should be sufficiently numerous and represent different areas of knowledge,
- selected people should be characterized by independent thinking and have different visions of the future.

The most popular heuristic method, known and used since 1938, is *brainstorming*. It is a universal technique for generating a large number of new ideas and choosing the best ones. The manner of its implementation and numerous modifications have been widely described in literature, so it will not be discussed in detail here.

A similar range and application has the so-called *Delphi method*, developed by a group of researchers from the Research and Development Corporation in Santa Monica (USA) in 1963. The expert team should include at least 20 outstanding specialists. There is no need for contact between experts, so they can live far away from each other. The composition of expert teams can be anonymous (at least until the time publication of results). The Delphi method in its classic form contains two rounds, and its more recent modifications may have a multi-stage character.

Usually, the purpose of the method is to study expert opinions on the probability or timing of future events occurrence. The main features of the method can be reduced to four requirements:

- independence of expert opinions,
- anonymity of their statements,
- multi-stage proceeding,
- agreeing and summarizing opinions of all experts.

By determining the forecast the highest probability rule is applied. The degree of compliance of experts' opinions for individual questions is characterized by means of such volatility measures as:

- dispersion factor of relative qualifications

$$h_r = \frac{k}{k-1} \left(1 - \sum_{j=1}^k f_{rj}^2 \right) \quad (5.12)$$

where:

- k number of categories distinguished in the r -rth question,
- f the frequency of j -th category in r -th question.

- concordance rate

$$W = \frac{12S}{n^2(k^3 - k)} \quad (5.13)$$

$$S = \sum_{j=1}^k \left(\sum_{i=1}^n x_{ij} - x_m \right)^2 \quad (5.14)$$

$$x_m = \frac{1}{k} \sum \sum x_{ij} \quad (5.15)$$

where:

- n number of experts,
- x_{ij} assessment of the j -th category by the i -th expert,

The concordance rate W assumes values from the numerical range $[0, 1]$, and its large (close to 1) value indicates high compliance of experts' opinions. The Delphi method is effective in situations characterized by low dynamics of changes, in other cases the concordance rate indicates a significant divergence of expert views, therefore the value of the forecast is doubtful.

The *cross-influences method*, otherwise known as the mutual interactions method, allows to assess the average probability of occurrence and the date of each of the events in the set of interdependent events, taking into account different possible order of events and its occurrence or not occurrence in the set of possible events. Among the various types of event linkages, only the combined events (occurring jointly) are included in the cross-flow method. The purpose of the

cross-influences method is to determine the average probabilities of individual events, taking into account the cumulative impact of all other events from the set.

The implementation procedure of the method consists of four stages:

- formulating the problem,
- selection of possible future events,
- building a cross-impact model,
- interpretation of results.

Scenario methods are to determine what situations may occur in the future as a consequence of each hypothetical possible events. The scenario may have a research (explorative) or anticipatory character. If the connections are of an explanatory nature, the scenario is of a research nature and determines what the effects will be for a given set of causes. If the relationships have the nature of effects, then the scenario is anticipatory and determines what the causes of this effects might have been.

The scenario may be descriptive or normative. The descriptive scenario only specifies the ordered sequence of possible events, omitting the assessment of whether they are desirable events or not. The scenario is normative if the goals and interests of the process owner are taken into account. Usually, scenario design takes place in seven steps, namely:

- Defining a research object, its elements and connections between them;
- Identifying phenomena belonging to the environment of a given object;
- Quantitative description of connections (relations) between elements of an object;
- Creating forecasts for variables belonging to the environment of the object;
- Development of pre-scenarios;
- Identification of factors interfering with the development process of the facility;
- Drawing up the final scenario design.

Scenario methods are particularly useful in forecasting processes and events related to the occurrence of risk, so they will be used in the next section.

5.5 Modelling of Disturbances in Logistic Network— Event Driven Approach

5.5.1 Identification of Sources of Risk, Threats and Hazards

The starting point to define a threat is a generalized risk concept, which is understood as a potential possibility of realising an undesirable scenario or event associated with the occurrence of negative consequences. The source of risk is a factor or an agent that alone or in combination with other agents has the potential to create possibilities of specific consequences. A threat is referring to the source of risk if its

consequences may cause a material damage (e.g. damage or destruction of infrastructure). However, hazard is a source of risk whose potential consequences concern safety (e.g. threats to human life or health).

In professional literature, many attempts have been made to classify sources of risk occurring in supply chains that are more or less universal in its nature. The most general is the classification recommended by the Federal Emergency Management Agency (FEMA P-789 [2013](#)), according to which sources of risk are divided into three main categories: external, internal and process-related ones. Based on this classification, we propose the following division of potential threats and hazards:

A. External sources of risk

a. Explosions

- nuclear attack or detonation,
- radiological attack (e.g. dirty bomb),
- explosives attack.

b. Biological attack

- aerosol anthrax; plague; ricin,
- food contamination,
- animal diseases (e.g. foot and mouth disease).

c. Pandemic influenza

d. Chemical attack or accident

- blister agent,
- nerve agent (paralyzing the nervous system),
- toxic industrial chemicals,
- chlorine tank explosion.

e. Infrastructure damage (critical infrastructure attack or failure)

- power failure (blackout),
- communication system failure or disruption,
- water supply contamination,
- sewage system failure,
- heating, ventilation and air conditioning systems failure,
- major fire.

f. Cyber-attack

- loss of data,
- computer network outage.

g. Economic and social

- economic catastrophe (market crash, loss of trust),
- demonstrations, riots and civil unrest,

- labour dispute,
- mass transit strike.

h. Natural disasters

- high winds (hurricane, tornado),
- winter storm,
- thermal anomalies
- major earthquake
- flood,
- tsunami,
- volcano eruption.

B. Internal sources of risk

- Sabotage,
- planning errors,
- computer system failure,
- lack of competence,
- crew dissatisfaction.

C. Process sources of risk

- inadequate critical supply,
- errors of partners or suppliers,
- incorrect process configuration,
- single points of failure.

The above-mentioned sources of risk are related to the causes of possible threats and hazards that concern the basic resources of the organization, namely: human, financial, intangible and infrastructural. This perspective, called the *resource approach*, can be the basis for classifying hazards and dangers also in logistics networks. On the basis of literature and our own works, we propose the following division of threats and dangers in relation to logistic networks:

A. Perspective of human resources

External threats

- explosive (nuclear, radiological, bomb attacks),
- biological attacks (diseases, poisoned food and water, epidemics and pandemics),
- chemical attacks and catastrophes (toxic, burning, explosive, paralyzing agents),
- social related (strikes, anxieties, riots, demonstrations).

Internal threats

- sabotage,
- planning mistakes,
- lack of competence.

B. The perspective of financial resources

External threats related to:

- market (dependence of prices on the market),
- currency (exchange rate changes),
- interest rate (changes in interest rates on the market),
- purchasing power (the impact of inflation on the purchasing power of the currency),
- politics (resulting from political decisions).

Internal threats related to:

- finance (resulting from liabilities to foreign capital),
- business (related to the changeability of income earned),
- financial liquidity (related to the fulfilment of contractors' obligations),
- transaction (non-compliance with the terms of the transaction).

C. Perspective of intangible assets

- theft of know-how,
- loss of key information.

D. Perspective of infrastructure resources

External threats

- power network failure
- transport system failure,
- water supply failure,
- telecommunications system failure.

Internal threats

- damage to the internal infrastructure (storage and warehousing facilities, transshipment terminals, ports, logistics centres),
- computer system failure.

5.5.2 Modelling of Exposures in Logistics Networks

Properly designed logistics networks are protected against potential threats and dangers by security systems consisting of various types of barriers. Therefore, real exposure to logistic networks are only those threats and hazards that have not been 'stopped' by their security systems. For modelling these exposures we propose to use a criterion based on the level of predictability of these events in order to classify these exposures. According to this criterion exposure may be:

- predictable by probabilistic methods—single events and chains of events,
- unpredictable by probabilistic methods—exceptional events as well as unknown phenomena and scenarios.

Below we will discuss both approaches sequentially.

5.5.2.1 Modelling of Exposures Predictable with Probabilistic Methods

Repeatable exposures may occur in the form of individual events or event chains leading to a destructive event, which may result in the loss of the continuity of the logistics network. These exposures are usually of a random nature and can be modelled in the form of random processes. A *random process* (RP) may be defined as an ensemble of given time functions, any one of which might be observed on any trial of an experiment or real process realization. The ensemble may include a finite number, a countable infinity, or a non-countable infinity of such functions. We will denote the ensemble of functions by $\{X(t)\}$, and any observed member of the ensemble by $x(t)$. The value of the observed member of the ensemble at a particular time t_i , is a *random variable*; on repeated trials of the experiment, $x(t_i)$ takes different random values. The probability that $x(t_i)$ takes values in a certain range is given by the *probability distribution function* (PDF), as it is for any random variable. Random process can be continuous or discrete (Joyce 2016; Montgomery and Runger 2003; Ross 2004; Scheaffer et al. 2011; Soong 2004).

Real random process, also called *stochastic process* (e.g. noise source), can be characterized by its properties, e.g. probability distribution function (PDF), cumulative distribution function (CDF), mean (expected value), variance, auto-correlation function (statistical average of the product of random variables), and cross-correlation function (measure of correlation between sample function amplitudes of processes $x(t)$ and $y(t)$ at time instants t_1 and t_2). We can characterize random processes based on how their statistical properties change. If the statistical properties of a random process RP don't change with time we call the RP *stationary*. The computation of statistical averages (e.g. mean and autocorrelation function) of a random process requires an ensemble of sample functions (e.g. data records) that may not always be feasible. However, to calculate the averages from a single data record is possible only in certain random processes called *ergodic processes*. The ergodic assumption implies that any sample function of the process takes all possible values in time with the same relative frequency that an ensemble will take at any given instant.

We distinguish three main random processes, which form the basis for modelling various phenomena occurring in engineered systems: the Bernoulli process, the Poisson process, and the Gaussian process. Other typical random processes are derived from these three processes as generalizations or specific cases (e.g. Markov process). Below we will briefly discuss these three random processes and the

resulting probability distributions of random variables that are applicable to modelling of typical exposures (based on Joyce 2016).

A. The Bernoulli random process

A single trial for a *Bernoulli process*, called a Bernoulli trial, ends with one of two outcomes, one called success (e.g. occurrence of the event E), the other called failure (e.g. no event E occurrence). Success occurs with probability p while failure occurs with probability $q = 1 - p$. The Bernoulli process consists of repeated independent Bernoulli trials with the same parameter p . These trials form a random sample from the Bernoulli population. If we ask how many successes there will be among n Bernoulli trials, then the answer will have a binomial distribution, *Binomial*(n, p). The Bernoulli distribution, *Bernoulli*(p), simply says whether one trial is a success. If we want to know how many trials it will be to get the first success, then the answer will have a geometric distribution, *Geometric*(p). If the question is how many trials there will be to get the r -th success, then the answer will have a negative binomial distribution, *Negative Binomial*(p, r). Given that there are M successes among N trials, if we ask how many of the first n trials are successes, then the answer will have a *Hypergeometric*(N, M, n) distribution. All these distributions are discrete, whereas the comparison of formulas for calculating their distribution models, mean values and variances is shown in Table 5.2.

B. The Poisson random process

A *Poisson process* is the continuous version of a Bernoulli process. In the Bernoulli process, time is discrete, and at each time unit there is a certain probability p that event occurs, the same probability at any given time, and the events at one time instant are independent of the events at other time instants. In the Poisson process, time is continuous variable, and there is a certain rate λ of events occurring per time unit that is the same for any time interval, and events occur independently of each other. Whereas in a Bernoulli process either no or one event occurs in a unit

Table 5.2 Formulas for calculating distribution models and parameters for discrete variables

Distribution	PDF	Mean	Variance
Bernoulli(p)	$f(0) = 1 - p; f(1) = p$	p	$p(1 - p)$
Binominal(n, p)	$f(x) = \binom{n}{x} p^x (1 - p)^{n-x},$ for $x = 0, 1, \dots, n$	np	$np(1 - p)$
Geometric(p)	$f(x) = p(1 - p)^{x-1},$ for $x = 1, 2, \dots$	$1/p$	$(1 - p)p^2$
NegativeBinominal(p, r)	$f(x) = \binom{x-1}{r-1} p^r (1 - p)^{x-r},$ for $x = r, r+1, r+2, \dots$	r/p	$r(1 - p)p^2$
Hypergeometric(N, M, n)	$f(x) = \binom{M}{x} \binom{N-M}{n-x} / \binom{N}{n},$ for $x = 0, 1, \dots, n$	np	$\binom{N-n}{N-1} npq$ for $q = 1 - p$

Table 5.3 Formulas for calculating distribution models and parameters for continuous variables

Distribution	PDF	Mean	Variance
Poisson(λ, t)	$f(x) = \frac{1}{x!} (\lambda t)^x e^{-\lambda t}$ for $x = 0, 1, 2, \dots$	λt	λt
Exponential(λ)	$f(x) = \lambda e^{-\lambda x}$ for $x \in [0, \infty)$	$1/\lambda$	$1/\lambda^2$
Gamma(λ, r)	$f(x) = \frac{1}{\Gamma(r)} \lambda^r x^{r-1} e^{-\lambda x}$ for $x \in [0, \infty)$	r/λ	r/λ^2
Beta(α, β)	$f(x) = \frac{1}{B(\alpha, \beta)} x^{\alpha-1} (1-x)^{\beta-1}$	$\frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}$	

time interval, in a Poisson process any nonnegative whole number of events can occur in a time unit. As in a Bernoulli process, we can ask various questions about a Poisson process, and the answers will have various distributions. If the problem is how many events occur in an interval of the length t , then the answer will have a Poisson distribution, *Poisson*(λt). If the question is how long until the first event occurs, then the answer will have an exponential distribution, *Exponential*(λ). If we ask how long until the r -th event, then the answer will have a gamma distribution, *Gamma*(λ, r). If there are $\alpha + \beta$ events in a given time interval, and the problem is what fraction of the interval it takes until the α -th event occurs, then the answer will have a beta distribution, *Beta*(α, β). All these distributions are continuous, whereas the comparison of formulas for calculating their distribution models, mean values and variances is shown in Table 5.3.

C. The Gaussian random process

A *Gaussian process* is a stochastic process, such that every finite collection of those random variables has a multivariate normal distribution, i.e. every finite linear combination of them is normally distributed. Its distributions are related to the central limit theorem which says that sample means and sample sums approach normal distributions if the sample size approaches infinity.

The normal distribution, *Normal*(μ, σ^2), also called the Gaussian distribution, is ubiquitous in probability and statistics. The parameters μ and σ^2 are real numbers, σ^2 being positive with positive square root σ called standard deviation. The standard normal distribution has $\mu = 0$ and $\sigma^2 = 1$. Normal distributions are used in statistics to make inferences about the population mean when the sample size n is large, and in Bayesian statistics as conjugate priors for the family of normal distributions with a known variance.

χ^2 -distribution, *ChiSquared*(v), is continuous. The parameter v , the number of ‘degrees of freedom’, is a positive integer. This is the distribution for the sum of the squares of v independent standard normal distributions. A χ^2 -distribution is a special case of a gamma distribution with a fractional value for r (*ChiSquared*(v) = *Gamma*(λ, r) where $\lambda = 1/2$ and $r = v/2$). χ^2 -distributions are used in statistics to make inferences on the population variance when the population is assumed to be normally distributed.

Student's T-distribution, $T(v)$, is continuous. If Y is $Normal(0, 1)$ and Z is $ChiSquared(v)$ and independent of Y , then $X = Y/(Z/v)^{1/2}$ has a $T(v)$ -distribution with v degrees of freedom. T-distributions are used in statistics to make inferences on the population variance when the population is assumed to be normally distributed, especially when the population is small.

Snedecor-Fisher's F-distribution, $F(v_1, v_2)$, is continuous. If Y and Z are independent χ^2 -random variables with v_1 and v_2 degrees of freedom, respectively, then $X = (Y/v_1)/(Z/v_2)$ has an F-distribution with (v_1, v_2) degrees of freedom. Note that if X is $T(v)$, then X^2 is $F(1, v)$. F-distributions are used in statistics when comparing variances of two populations. All these distributions are continuous. Formulas for calculating distribution models and parameters for normal and χ^2 -distribution as well as other selected distributions is shown in Table 5.4.

In practice, probability distributions that are not derived from these random processes can be also used to model rare events, and in particular their maximum values. These are mainly distributions based on the extreme value theory as well as those that relate to the distribution of rank data frequencies. *Extreme values distributions* are based on statistics constructed on time series of random samples taken at identical time intervals, in long time intervals, from which samples only extreme values (maximum or minimum) are used. In the case of exposure modelling, the maximum values characterizing the given exposure parameter are especially important, therefore the Gumbel distribution can be a useful model, provided that observations or measurements are available from a sufficiently long time interval (Gumbel 1941). It should be emphasized that the expected value of the

Table 5.4 Formulas for calculating distribution models and parameters for normal- and other selected distributions

Distribution	PDF	Mean	Variance
Normal(μ, σ^2)	$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$ for $x \in \mathbb{R}$	μ	σ^2
LogNormal(μ, σ)	$f(x) = \frac{1}{x\sigma\sqrt{2\pi}} \exp\left(-\frac{(\ln(x)-\mu)^2}{2\sigma^2}\right)$ for $x \in [0, \infty)$	$e^{\mu + \sigma^2/2}$	$(e^{\sigma^2} - 1)e^{2\mu + \sigma^2}$
ChiSquared(v)	$f(x) = \frac{x^{\frac{v}{2}-1} e^{-x/2}}{2^{\frac{v}{2}} \Gamma(\frac{v}{2})}$, for $x \geq 0$	v	$2v$
Uniform(n) discrete	$f(x) = 1/n$, for $x = 1, 2, \dots, n$	$(n+1)/2$	$(n^2-1)/12$
Uniform(a, b) continuous	$f(x) = 1/(b-a)$, for $x \in [a, b]$	$(a+b)/2$	$(b-a)^2/12$
Triangular(a, b, c)	$f(x) = \frac{2(x-a)}{(b-a)(c-a)}$ for $a \leq x \leq c$ $f(x) = \frac{2(b-x)}{(b-a)(b-c)}$ for $c \leq x \leq b$	$\frac{a+b+c}{3}$	$\frac{a^2+b^2+c^2-ab-ac-bc}{18}$
Weibull(α, β)	$f(x) = \frac{\beta}{\alpha} \left(\frac{x}{\alpha}\right)^{\beta-1} e^{-\left(\frac{x}{\alpha}\right)^\beta}$ for $x > 0; \alpha > 0; \beta > 0$	$\alpha \Gamma\left(1 + \frac{1}{\beta}\right)$	$\alpha^2 \Gamma\left(1 + \frac{2}{\beta}\right) - \alpha^2 \Gamma^2\left(1 + \frac{1}{\beta}\right)^2$

extreme increases with the length of the time segment it concerns. A classic example of the practical and effective use of this model to predict possible floods in Black Canyon on the Colorado River is the work of Gumbel from 1941.

The term *Zipf's law* refers to frequency distributions of rank data. Originally, Zipf's law stated that, in natural language utterances, the frequency of any word is roughly inversely proportional to its rank in the frequency table. So, the most frequent word will occur approximately twice as often as the second most frequent word, which occurs twice as often as the fourth most frequent word, etc. (Hawa 2007). The power distribution was created as a generalization of Pareto diagrams known for a long time and the Zipf's law. Professor of German Studies at the Harvard University Georg Kingsley Zipf stated that the distribution of the frequency of individual words in different languages (especially English) is subject to the simplest form of power distribution with an exponent equal to -1 . In later studies, this distribution has proved particularly useful in the practice of modelling single random events, in particular such as natural disasters (earthquakes, forest fires, etc.). General model in the simplest form can be presented as following:

$$Y = ax^b \quad (5.16)$$

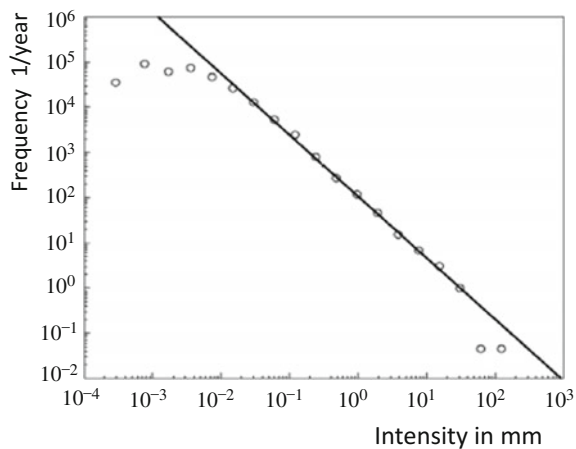
which after nonlinear transformation can be presented in the form of a linear relationship

$$y' = c + bx' \quad (5.17)$$

where: $y' = \log y$; $x' = \log x$; $c = \log a$

In applications where the description of the scale (size) of an event is significant, the exponent b must have a negative value. An example of a graphical representation of dependencies described by the power model with the exponent $b = -0.4$ is shown in Fig. 5.14.

Fig. 5.14 Distribution of rainfall frequency as a function of their intensity (Somette 2009)



Summing up, it can be concluded that the prediction of exposures with the nature of single, repetitive events is currently not a major problem, and the IT tools supporting the quantitative assessment of random variables parameters are widely available.

The *chains of events* leading to the loss of the logistic processes continuity could theoretically be modelled by simple probabilistic dependencies or using stochastic processes, in particular the so-called Markov and Semi-Markov processes. These models have been described in detail in the literature (Eberle 2015), therefore they will not be discussed in detail in this paper. However, in practice most of the assumptions underlying these models are not met, so the usability of these models is in many cases limited.

5.5.2.2 Modelling of Exposures Unpredictable with Probabilistic Methods

Heuristics and analogue type models, e.g. based on metaphors, are becoming more and more popular in this area. The most common of these are:

- a domino model,
- a model of Swiss cheese,
- a pyramid safety model,
- a functional resonance model,
- a model of a perfect storm.

In the classic domino model, it is assumed that the end event (unfavourable) is the effect of successive events, each of which is the result of a previous event and the cause of the next event. This model was proposed by H. Heinrich (1959) on the assumption that successive events form a causal chain leading to an accident. Currently, it is used, among others for modelling the so-called cascading failures.

The model of Swiss cheese, also known as the James Reason (1997) model, was created on the assumption that an unfavourable final event occurs as a result of overlapping of distortions, errors and mistakes at various stages of the process. As a rule, it is assumed that the exposure is the result of a combination of events in the area of technology, environment, human factor and management. Some authors associate the Reason model with so-called Murphy's law, from which it follows that if there is only a potential possibility of an adverse event, it will happen sooner or later. An example of a graphic interpretation of the Reason model for the development of the situation of exposures leading to a disaster is shown in Fig. 5.15.

The safety pyramid model is a development of Heinrich's concept, who noticed that there were 30 incidents (minor accidents) and one serious accident in about 300 dangerous situations (Heinrich 1959). These proportions have been questioned in later studies, but the idea is developed into a model that is commonly used in cases where human errors are the main cause of disturbances leading to exposures. An example of a safety pyramid developed by the International Atomic Energy Agency (IAEA) to assess the scale of nuclear exposures (INES—International Nuclear Event Scale) is shown in Fig. 5.16.

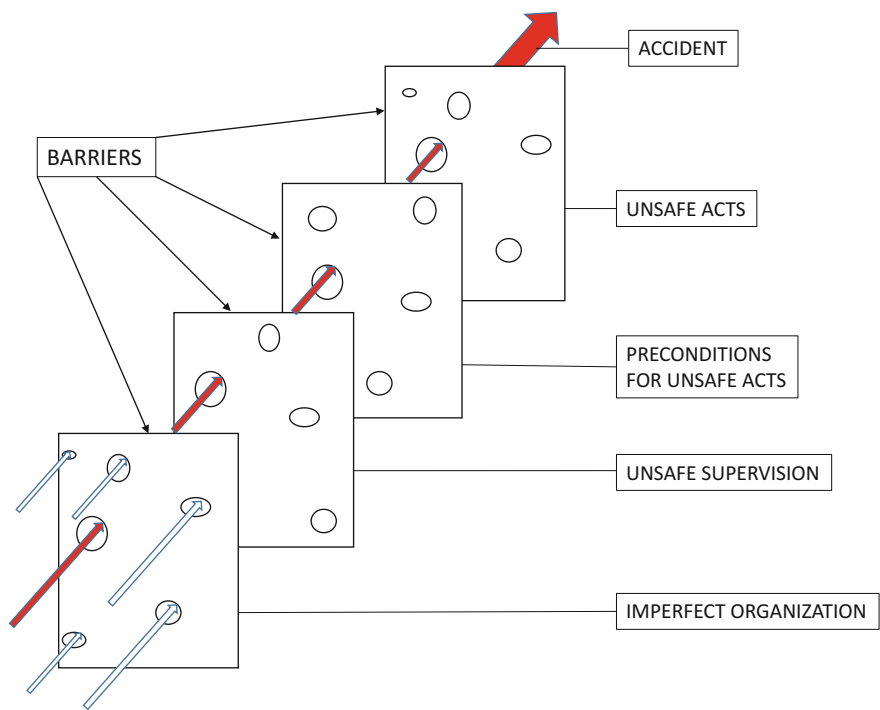


Fig. 5.15 An example of using a Swiss-cheese model to describe the process of developing exposures leading to an accident

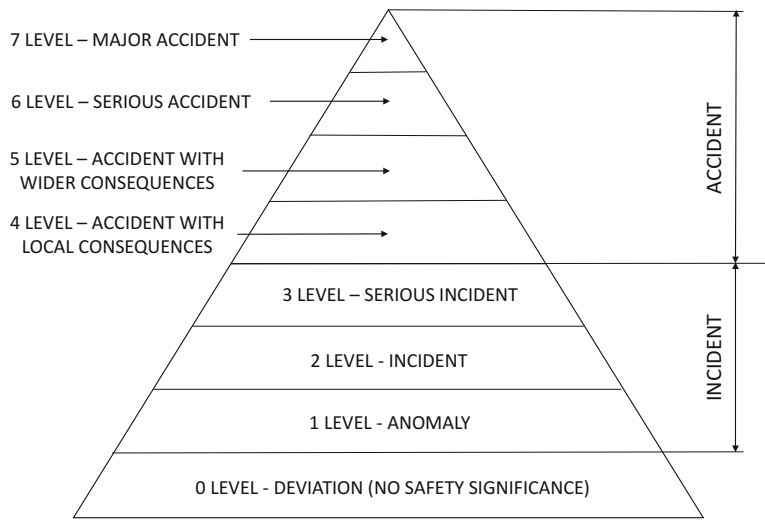
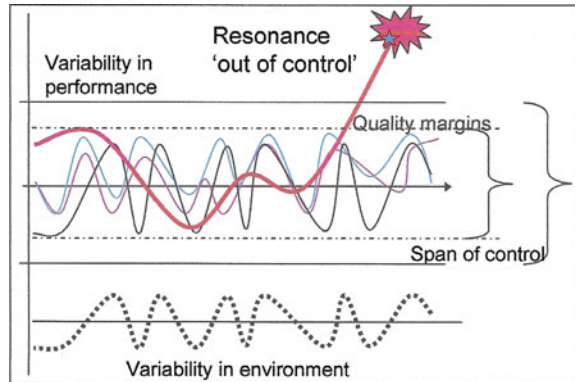


Fig. 5.16 Safety pyramid as a model of exposures scale according to the International Atomic Energy Agency (based on Spiegelberg-Planer 2009)

Fig. 5.17 An example of a graphical interpretation of the FRAM model (based on Hollnagel et al. 2006)



The resonance analogy was used by Erik Hollnagel (Hollnagel et al. 2006) to propose a Functional Resonance Analysis Method (FRAM), and the functional resonance model. Figure 5.17 shows an example of the FRAM model interpretation for a certain system, described by many parameters subjected to random changes (in the figure, the time courses of three selected parameters are shown with thin lines). The behaviour of the entire system (presented in the figure in the form of a time course with a thick line) is a resultant of the instantaneous values of individual system parameters and the impact of the environment (in the drawing presented in simplified form as a single waveform with a dotted line). A characteristic feature of functional resonance phenomena is that a particularly unfavourable (and very rarely occurring) configuration of system parameters and ambient values can lead to a significant exceeding of the allowable parameter describing the entire system, while its individual and surrounding parameters remain constant within the limits of acceptable changes.

The metaphor of the ‘perfect storm’ was based on an analogy to the real catastrophic event that occurred in 1991 in the Atlantic, off the coast of the USA. The Perfect Storm—Halloween Nor’easter consumed 13 deaths, resulting from the combination of three phenomena: the hurricane ‘Grace’, which slowly faded over the Atlantic, a newly developing storm not too far from it and a great atmospheric front from the Great Lakes. The energy from the front and the new storm caused that the ‘dying’ hurricane was reborn, becoming a new hurricane of unprecedented strength and speed. The ‘ideal storm phenomena’ are, therefore, the result of exceptionally unfavourable coincidences of circumstances that are not separately analysed in themselves, and together they create a new, very difficult to predict scenario, leading to a non-linear (often exponentially) accumulation of the final effect (Pate-Cornell 2012).

It is much more difficult to predict exposures that occur very rarely and whose effects can be very negative. These are so-called LSLIRE events (Large Scale, Large Impact, Rare Event), which may be exceptional phenomena due to their scale and due to the lack of historical data about the possibility of their occurrence.

In these cases, the heuristic methods discussed in Sect. 5.4.2 as well as metaphors like ‘dragon-kings’ and ‘black swans’ can be helpful.

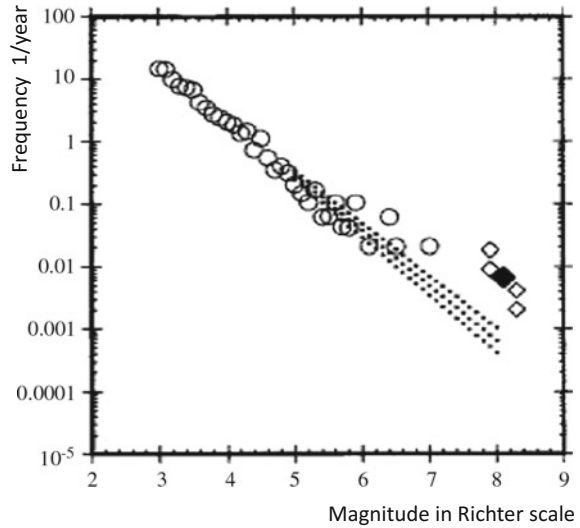
‘Black Swan’ phenomena are characterized by the following features: uniqueness that goes beyond expectations based on previous experience, extremely large event effects and the possibility of explaining the reasons only after the occurrence of these threats (a posteriori). An additional difficulty is the so-called ‘Aggregation of risks’ characterized by, among others: the possibility of simultaneous occurrence of two or more serious events caused by various causes, mutual impact of risk events and accumulation of risks, with a nonlinear nature (a multiplicative model instead of an additive one). The reason for the existence of this type of phenomena is usually the imperfect knowledge of decision makers about possible threats, or an error consisting in the lack of imagination by thinking based on analogies.

The author of the ‘black swan’ metaphor, Nassim Nicholas Taleb, focuses in his books (Taleb 2010, 2013) on searching for effective remedies for LSLIRE phenomena, and introduces the concepts of ‘fragility’ and ‘antifragility’ as synonyms of vulnerability and resistance to the phenomena of the ‘black swan’ and ‘perfect storm’ nature. He assumes that in the case of complex engineered systems there are many implicit relations between the components of these systems, which results in their behaviour non-linearity, and sometime the release of reaction chains—so-called cascading failures. He concludes that all attempts to create prediction models that allow forecasting LSLIRE phenomena with satisfactory accuracy fail in practical applications, and suggests focusing on actions aimed at reducing the ‘fragility’ of the system components to the minimum and striving to maximize the ‘antifragility’ of entire systems.

According to the author of this work, the introduction of the concepts of ‘fragility’ and ‘antifragility’ in the context of assessing the complex engineered systems vulnerability to this kind of threats could lead to ambiguity due to the commonly accepted in technical sciences understanding of the concept of fragility (especially in materials science and mechanical engineering). On the other hand, the thesis about the low usefulness of prognostic models, especially those based on mathematical statistics and probability calculus, to assess the risk of losing the ability to perform the required functions of large scale systems as a result of LSLIRE events is right.

The metaphor of ‘dragon-kings’ refers to phenomena that are known and predictable regarding the potential possibility of their occurrence, but not adequate to the remaining values of the whole set. The concept of this metaphor was built on the ground of incompatibility of some very rare but repetitive events of the type of natural disasters, with the power model, which in the vast majority of cases was completely consistent with the observed facts. The classic statistical approach calls these observations ‘fatal errors’ (outliers) and assumes that they are the results of mistakes or errors in the measurement process or by data processing. However, long-term research on earthquakes and other natural disasters has shown that these outliers are often real results, not burdened with fatal errors and belong to the so-called thick tails of accepted probability distributions, for which theoretically it is impossible to define a variance.

Fig. 5.18 The distribution of the earthquake magnitude in California at the San Andreas Fault (based on Sornette 2009)



It was found that in most cases the scale of a natural disaster can be described by models (5.16) and (5.17) with the exponent b with values ranging from -0.3 to -0.7 , while a small part of events significantly deviates from this model and indicates their membership in the distribution with different parameter. The explanation for this phenomenon may be some processes occurring in the so-called ‘critical points’, such as the Curie point in so-called ferromagnetic materials, percolation (the process of water flow through a solid substrate that elutes or precipitates the substance), or the so-called self-organized criticality (SOC). These processes may be the result of phase transformations, bifurcations (in chaotic systems), and the existence of so-called tipping points. An example of self-organized criticality are all kinds of landslides (terrestrial and mud) as well as avalanches. Also, a sufficiently large sand pile evolves itself in the direction of a critical condition, in which even a minimum disturbance can cause the whole pile to slip-down rapidly. Figure 5.18 shows an example of the earthquake magnitude frequency in San Andreas (California). At the picture we can see that only five cases with the highest magnitude (‘dragon-kings’) definitely deviate from the distribution model for the several dozen quantified cases.

References

- Albar FM, Jetter AJ (2009) Heuristics in decision making. In: PICMET 2009 proceedings, Portland, Oregon USA, 2–6 Aug 2009
- Angerhofer BJ, Angelides MC (2000) System dynamics modelling in supply chain management: research review. In: Joines JA, Barton RR, Kang K, Fishwick PA (eds) Proceedings of the 2000 winter simulation conference, pp 342–351

- AnyLogic (2018) <http://www.anylogic.com/features>
- APQC (2015) APQC's process classification framework version 6.1.1. https://www.qgcio.qld.gov.au/_data/assets/pdf_file/0026/5894/APQC_PCF_Ver_6.1.1-final-1.pdf
- ARIS (2018) <https://www.ariscommunity.com/>
- Arnold D (1995) Materialflusslehre. Vieweg, Braunschweig
- Barbati M, Bruno G, Genovese A (2011) Applications of agent-based models for optimization problems: a literature review. *Expert Syst Appl* 39(5):6020–6028
- Birta LG, Arbez G (2007) Modelling and simulation exploring dynamic system behaviour. Springer, London
- Bonabeau E (2001) Agent-based modeling: methods and techniques for simulating human systems. *Proc Natl Acad Sci* 99(3):7280–7287
- Bonabeau E, Dorigo M, Theraulaz G (1999) Swarm intelligence: from natural to artificial systems. Oxford University Press, Oxford
- Booch G, Jacobson I, Rumbaugh J (2005) The unified modeling language user guide, 2nd edn. Addison-Wesley, Boston
- Borshchev A, Filippov A (2004) From system dynamics and discrete event to practical agent based modeling: reasons, techniques, tools. In: The 22nd international conference of the system dynamics society, 25–29 July 2004, Oxford, England. https://www.systemdynamics.org/assets/conferences/2004/SDS_2004/PAPERS/381BORSH.pdf
- BPMN Tutorial (2018) <https://camunda.com/bpmn/>
- Bukowski L (1995) Statistische Methoden im Ingenieurwesen. Verlag der Technischen Universität Clausthal
- Bukowski L, Karkula M (2003) The simulation of logistic processes using DOSIMIS-3 simulator. In: Proceedings of the international conference on logistics, Ostrava, pp 296–300
- Bukowski L, and Karkula M. (2009) Modelling and simulation of logistics processes in heat and power plants—a hybrid approach. In: Proceedings of the twentieth international conference on systems engineering—ICSE 2009, Coventry, United Kingdom. ISBN 978-1-84600-0294
- Bukowski L, Karkula M (2010) Integration of discrete event simulation, decision tables and fuzzy systems in modelling of logistics processes. In: Advances in systems science. Academic Publishing House EXIT, pp 113–121
- Cassandras CG, Lafortune S (2009) Introduction to discrete event systems. Springer, Berlin
- Cochran JK, Mackulak GT, Savory PA (1995) Simulation project characteristics in industrial settings. *Interfaces* 25(4):104–113
- DFD (2018) <https://www.lucidchart.com/blog/data-flow-diagram-tutorial>
- Eberle A (2015) Markov processes. https://wt.iam.uni-bonn.de/fileadmin/WT/Inhalt/people/Andreas_Eberle/MarkovProcesses/MPSkript1415.pdf
- EPC (2018) <https://www.ariscommunity.com/event-driven-process-chain>
- ERD (2018) <https://www.lucidchart.com/pages/er-diagrams>
- FEMA P-789 (2013) Continuity guidance circular 2. Continuity guidance for non-federal governments: mission essential functions identification process (states, territories, tribes, and local government jurisdictions). <https://ready.alaska.gov/Plans/continuity/Continuity-Guidance-Circular2.pdf>
- Fishman GS (2001) Discrete-event simulation: modeling, programming, and analysis. Springer, Berlin
- Forecast Sheets in Excel 2016—Tutorial (2016) <https://www.teachucomp.com/forecast-sheets-in-excel-2016-tutorial/>
- Forrester JW (1958) Industrial dynamics: a major breakthrough for decision makers. *Harvard Bus Rev* 36(4):37–66
- Forrester JW (1961) Industrial dynamics. Productivity Press, Portland
- Gigerenzer G, Gaissmaier W (2011) Heuristic decision making. *Annu Rev Psychol* 62:451–482
- Gilbert N, Troitzsch K (2005) Simulation for the social scientist, 2nd ed. McGraw-Hill, GMU (George Mason University). MASON Home Page. <http://cs.gmu.edu/~eclab/projects/mason/>. Accessed 29 July 2014

- Gordon G (1961) A general purpose systems simulation program. In: Proceedings of EJCC, Washington D.C. McMillan, NY, pp 87–104
- Gumbel EJ (1941) The return period of flood flow. *Ann. Math. Stat* 12:163–190
- Hawa M (2007) Probability distribution summary. <https://www.google.com/search?ei=vnNTW-TNFsPKwAL217G4BQ&q>
- Heinrich HW (1959) Industrial accidents prevention. Mc Graw Hill Book Company Inc., New York
- Hollnagel E, Woods DD, Leveson N (2006) Resilience engineering: concepts and precepts. Ashgate, Aldershot
- <http://www.breezetre.com/article-exel-flowchart-shapes.htm>
- https://www.google.pl/search?q=aris+examples&biw=1644&bih=906&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwivic_na3qvKAhWDiiWKHZg2CMYQsAQIGg#imgsrc=6P2Wp74zly_iRM%3A
- <http://www.properformasimulation.co.uk/technology.html>
- Joyce D (2016) Common probability distributions Probability and Statistics. <https://mathcs.clarku.edu/~djoyce/ma218/distributions.pdf>
- Karkula M, Bukowski L (2012) Computational intelligence methods—joint use in discrete event simulation model of logistics processes. In: Laroque C, Himmelsbach J, Pasupathy R, Rose O, Uhrmacher AM (eds) Proceedings of the 2012 winter simulation conference, Berlin, © IEEE
- Law AM (2007) Simulation modeling and analysis, 4th edn. McGraw-Hill, New York
- Law AM, Kelton WD (1991) Simulation modelling and analysis. McGraw-Hill, Inc., NY
- Macal C (2004) Emergent structures from trust relationships in supply chains. In: Macal C, Sallach D, North M (2004) Proceedings of agent: conference on social dynamics, Chicago, IL, 7–9 Oct 743–760, Argonne National Laboratory
- Macal C, North M (2003) Effects of global information availability in networks of supply chain agents. In: Macal C, Sallach D, North M (eds) Proceedings of agent: conference on challenges in social simulation, Chicago, IL, Argonne National Laboratory, 2–4 Oct 2003, pp 235–252
- Macal C, North M (2006) Tutorial on agent-based modeling and simulation part 2: how to model with age. In: Perrone LF, Wieland FP, Liu J, Lawson BG, Nicol DM, Fujimoto RM (eds) Proceedings of the 2006 winter simulation conference, pp 73–83
- Macal C, North M (2010) Tutorial on agent-based modeling and simulation. *J Simul* 4(3):151–162
- Macal C, North M (2014) Introductory tutorial: agent-based modeling and simulation. In: Tolk A, Diallo SY, Ryzhov IO, Yilmaz L, Buckley S, Miller JA (eds) Proceedings of the 2014 winter simulation conference, pp 6–20
- Maria A (1997) Introduction to modeling and simulation. In: Andradóttir S, Healy KJ, Withers DH, Nelson BL (eds) Proceedings of the winter simulation conference 1997, pp 7–13. <http://acqnotes.com/Attachments/White%20Paper%20Introduction%20to%20Modeling%20and%20Simulation%20by%20Anu%20Maria.pdf>
- Montgomery DC, Runger GC (2003) Applied statistics and probability for engineers. Wiley, Hoboken
- Morecroft JDW (2015) Strategic modelling and business dynamics. A feedback systems approach. Wiley, New York
- NASA (2013) NASA-STANDARDS-7009. https://spaceflightsystems.grc.nasa.gov/SpaceDOC_II/Standards/documents/NASA-STD-7009.pdf
- NASA (2016) NASA-STANDARDS-7009a. <https://standards.nasa.gov/standard/nasa/nasa-std-7009>
- NetLogo (2006) NetLogo home page. <http://ccl.northwestern.edu/netlogo>
- Nyere J (2008) The design-chain operations model. <http://www.supply-chain.org>
- Pate-Cornell E (2012) On “black swans” and “perfect storms”: risk analysis and management when statistics are not enough. *Risk Anal* 11:1823–1833
- PETRI (2018) <https://www.google.pl/search?q=sieć+petriego&biw=1644&bih=906&tbm=isch&tbo=u&source=univ&sa=X&sqi=2&ved=0ahUKEwi90eGGhKrKAhXCCSwKHUIZDuoQsAQIKQ#imgdii=EKSPYGaTet6C>
- Reason J (1997) Managing the risks of organizational accidents. Ashgate, Aldershot, UK

- Robinson S (2008) Conceptual modelling for simulation part I: definition and requirements. *J Oper Res Soc* 59(3):278–290
- Ross SM (2004) Introduction to probability and statistics for engineers and scientists. Elsevier Academic Press, Cambridge
- Scheaffer RL, Mulekar M, McClave JT (2011) Probability and statistics for engineers. Cengage Learning, Brooks/Cole
- Scheer AW, Jost W, Heiss H, Kronz H (eds) (2006) Corporate performance management. ARIS in practice. Springer, Berlin
- SCOR (2018) <http://cloud.ld.ttu.edu/idu0010/Portals/0/Harjutustunnid/SCOR10.pdf>
- Seth D, Gupta V (2007) Application of value stream mapping for lean operations and cycle time reduction: an Indian case study. *Prod Plan Control* 16(1):44–59
- Soong TT (2004) Fundamentals of probability and statistics for engineers. Wiley, Hoboken
- Sornette D (2009) Dragon-kings, black swans and the prediction of crises. *Int J Terraspace Sci Eng*. <http://www.arxiv.org/physics>
- Spiegelberg-Planer R (2009) A matter of degree. A revised international nuclear and radiological event scale (INES) extends its reach. *IAEA Bull* 51–1:46–49. <https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull51-1/51102744649.pdf>
- Sterman JD (1989) Modeling managerial behavior: misperceptions of feedback in a dynamic decision making experiment. *Manag Sci* 35(3):321–339
- Sterman JD (2001) System dynamics modeling: tools for learning in a complex world. *California Manag Rev* 43(4):8–25
- Sterman JD (2000) Business dynamics: systems thinking and modeling for a complex world. Irwin McGraw-Hill, Boston
- Swaminathan J, Smith S, Sadeh N (1998) Modelling supply chain dynamics: a multiagent approach. *Decis Sci* 29(3)
- SWARM (2018) The swarm simulation system, a toolkit for building multi-agent simulations. <http://www.santafe.edu/projects/swarm/overview/overview.html>
- Sweetser A (2009) A comparison of system dynamics (SD) and discrete event simulation. <https://pdfs.semanticscholar.org/bca5/0943f66fd012dd62168433d5f04221b5d6f5.pdf>
- Taleb NN (2010) The black swan: the impact of the highly improbable. Penguin Books, London
- Taleb NN (2013) Antifragile. Things that gain from disaster. Penguin Books, London
- Wild R (2002) Operations management, 6th edn. Continuum, London
- Woodward WA, Gray HL, Elliott AC (2012) Applied time series analysis. CRC Press, Boca Raton
- Wooldridge M (2009) An Introduction to Multiagent Systems. John Wiley & Sons Ltd, Hoboken

Chapter 6

Assessment Operational Risk and Dependability of Logistic Networks—Application Examples



There are no such things as applied sciences, only applications of science.

Louis Pasteur

6.1 A Framework for Evaluation of Logistic Networks Operational Risk and Dependability—ELNORD

Based on the Chaps. 2–5 we propose a general framework for evaluation of logistic networks operational risk and dependability (ELNORD). It consists of 10 steps, and its simplified algorithm is shown in Fig. 6.1. The individual steps of the algorithm will be discussed below.

Step 1 Problem defining

The most common problem is to design a new logistics network or modify an existing one for specific requirements and restrictions. A so-called ‘System Engineering Process’ approach can be helpful in this respect (SEF 2001). The systems engineering process is a top-down comprehensive, iterative and recursive problem solving process, applied sequentially through all stages of development, that is used to:

- Transform needs and requirements into a set of system product and process descriptions, e.g. through concurrent consideration of all lifecycle needs,
- Ensure the compatibility, interoperability and integration of all functional and physical interfaces and make certain that system definition and design reflect the requirements for all system elements: hardware, software, facilities, people, and information,
- Generate information for decision makers to identify and characterize system’s vulnerabilities and technical risks.

The fundamental systems engineering process activities are: Requirements Analysis, Functional Analysis and Allocation, as well as Design Synthesis additionally balanced by techniques and tools called System Analysis and Control.

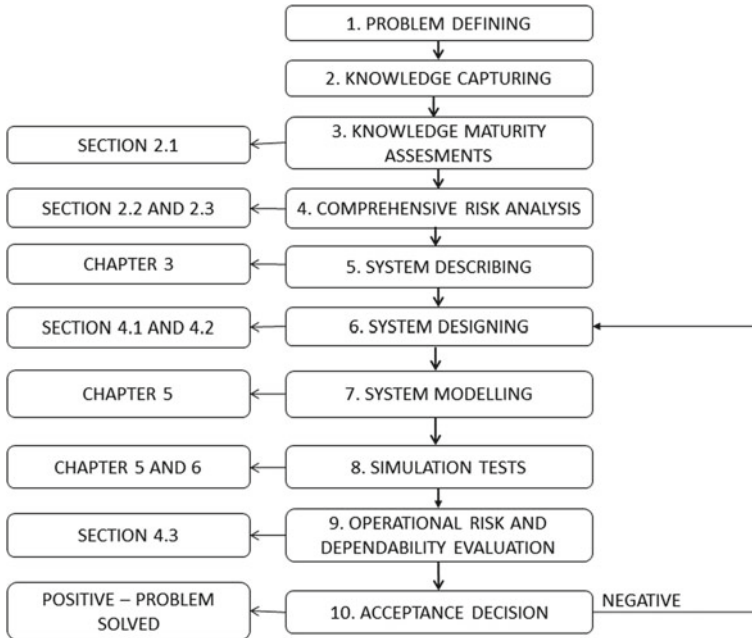


Fig. 6.1 The simplified algorithm of the framework for evaluation of logistic networks operational risk and dependability (ELNORD)

System Controls (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance—C4ISR) are used to track the correctness of the decision implementation and its compliance with the requirements. When defining the problem of the logistics network configuration, three main perspectives should be taken into account: functional, physical, and system architectures. The functional architecture identifies and structures the allocated functional and performance requirements. The physical architecture describes the system product by showing how it is broken down into subsystems and components. The system architecture identifies all the products (including enabling products) that are necessary to support the system and, by implication, the processes necessary for development, production, construction, deployment, operations, support, disposal, training, and verification.

The main inputs to the process include the customer's requirements and the project constraints. Requirements relate directly to the attributes of the system being designed, e.g. performance characteristics and operability related measures (see Sect. 3.3). They contain the stated life-cycle customer needs and objectives for the system, and they relate to the quality of the system operation in its intended environment. Constraints are conditions that exist because of limitations imposed by the environment, available resources, or technology. The process's primary purpose is to transform the requirements into designs within the constraints.

Typical categorizations of requirements that relate to engineering perspective are the following (SEF 2001):

- Customer requirements—statements of fact and assumptions that define the expectations of the system in terms of system objectives, environment and constraints. Operational requirements will define the basic need and measures of performance as well as operability of the system being designed.
- Functional requirements—the necessary task, action or activity that must be accomplished. Functional requirements identified in the requirements analysis should be used as the main functions for a functional analysis.
- Performance requirements—the extent to which a function must be executed; generally measured in terms of quantity, quality, coverage, timeliness or readiness. During requirements analysis, performance requirements should be interactively developed across all identified functions, and characterized in terms of the degree of certainty in their estimate, the degree of criticality to system success, and their relationship to other requirements.
- Design requirements—the so-called ‘build to’, ‘code to’, and ‘buy to’ requirements for products and ‘how to execute’ requirements for processes expressed in technical data sets and technical manuals.

Requirements analysis involves defining customer needs and objectives in the context of planned customer use, environments, and identified system characteristics to determine requirements for system functions. Prior analyses are reviewed and updated, refining mission and environment definitions to support system definition. Requirements analysis is conducted iteratively with functional analysis to optimize performance requirements for identified functions, and to verify that synthesized solutions can satisfy customer requirements. The purpose of requirements analysis is to refine customer objectives and requirements, and especially (SEF 2001):

- Define initial performance objectives and refine them into requirements;
- Identify and define constraints that limit solutions; and
- Define functional and performance requirements based on customer provided measures of effectiveness.

Requirements analysis should also result in a clear understanding of: functions (what the system has to do), performance (how well the functions have to be performed), interfaces (environment in which the system will perform), and eventually other requirements and constraints, specific for the system being designed,

A more detailed description related to defining the problem can be found in literature (e.g. SEF 2001).

Step 2 Knowledge capturing

The general model of knowledge creating process is shown in Fig. 2.3. The entire process is presented as a chain of operations and flows that are subjected to

disturbances. The raw data stored in Data Acquisition block is sent to the Data Processing block and subjected to the preparation process. The processed data flows to Data Verification block where they are verified for their veracity and then sent to Data Forming block for generation of Data Mining and Fusion of Data. Raw information flows to Information Evaluating block, where they are evaluated for their utility value and selected on this basis. The selected information is used in Building Patterns block to search for relationships between individual pieces of information and build logical patterns, based on which a new knowledge is generated in New Knowledge Creation block. The last stage of the chain is to enrich the existing knowledge base with new knowledge and to create initial knowledge for further acquisition of new data.

In order to ensure the quality of the information on which the new knowledge is created, the process of data preparation is of particular importance; thus it will be described in more detail. In data processing step four main tasks may be differentiated: data cleaning, data integration, data transformation, and data reduction. Section 2.1 contains more detailed analysis of capturing knowledge process with special stress on uncertainty of data and information as well as imperfection of the available knowledge.

Step 3 Knowledge maturity assessment

Assessment of the *knowledge maturity* (KM) should be based on three basic criteria, namely: data veracity value (five levels), information utility value (five levels) and knowledge processing quality (five levels). Methods for determining these criteria are described in Sects. 2.1.2 and 2.1.3. The whole process of assessing the maturity of knowledge based on imperfect data, information and knowledge processing can be presented in the form of the following algorithm:

(a) Data Veracity (DV) evaluation

DV is described by a five-dimensional vector of its attributes A_i : Accuracy (ACC), Clarity (CLA), Consistency (CON), Plausibility (PLA) and Traceability (TRA). Each veracity attribute A_i is rated on a 3-point scale as: 0—unacceptable, 1—acceptable, or 2—fully satisfactory, and on this basis, the *Data Veracity Value* (DVV) is calculated as the product of all five attributes A_i . The result of the assessment is to assign them to one of five classes, namely: very low (VL), low (L), moderate (M), high (H), or very high (VH). Data for which Data Veracity Value is very low ($DVV = 0$) should be eliminated and must not be used to create information (more details are given in Sect. 2.1.2).

(b) Information Utility (IU) evaluation

Information Utility (IU) is the property of the information described by a five-dimensional vector of its attributes B_i : Believability (BEL), Completeness (COM), Correctness (COR), Relevancy (REL), and Timeliness (TIM). Each IU attribute B_i is rated by experts on a 3-point scale as: 1—low, 2—moderate, 3—high, and on this basis the *Information Utility Value* (IUV) is calculated as the product of

all five attributes B_i . The result of the assessment is to assign them to one of five classes, namely: very low (VL), low (L), moderate (M), high (H), or very high (VH).

(c) Knowledge Processing Quality (KPQ) evaluation

Knowledge Processing Quality (KPQ) is the property of the knowledge creating process described by a five-dimensional vector of its attributes as follows: Model Type Adequacy (MTA), Model's Parameters Accuracy (MPA), Decision Making Process Correctness (DMC), Decision Communication Process Reliability (DCR), and Decision Realization Process Compliance (DRC). Each KPQ attribute C_i is rated by experts on a 3-point scale as: 1—low, 2—moderate, 3—high, and on this basis, the value of the *Knowledge Processing Quality* (KPQ) is calculated as the product of all attributes C_i . The result of the assessment is to assign them to one of five classes, namely: very low (VL), low (L), moderate (M), high (H), or very high (VH).

(d) Knowledge Maturity (KM) assessment

Each KM attribute D_i is rated on a 5-point scale, and on this basis, the value of the *Knowledge Maturity Level* (KML) is calculated as the product of all attributes A , B and C . Maturity of knowledge can also be assessed on five levels, e.g.: very low (insufficient) maturity level (VL), low maturity level (L), moderate maturity level (M), high maturity level (H), and very high (fully satisfactory) maturity level (VH). Very low (VL) maturity level can be identified with a lack of knowledge, the level L—weak imperfect knowledge, the level M—medium imperfect knowledge, the level H—strong imperfect knowledge, and the level VH—complete, perfect knowledge.

Step 4 Comprehensive risk analysis

The comprehensive risk analysis should include all three basic groups of risks, namely: opportunity related risks (covering the risk of lost and missed chances), hazard related risks (including risks in a safety context), and threat related risks (concerning risks of detriment). This last group contains economic risk (the potential of losing something of value such as financial wealth, e.g. financial, commercial and price risks) as well as technical risk (operational risk—risk in context of operation system unavailability, e.g. potential for realization of unwanted scenario leading to a disruptive event with possibility of negative consequences). The basis for conducting such a risk analysis may be Chap. 2, and especially Sects. 2.2 as well as 2.3 of this work.

Step 5 System describing

Describing engineered systems is the content of Chap. 3. A full description of the assessed system should be carried out both in terms of system and process approach using both topology- and flow-based methodology. The infrastructure description should pay particular attention to its complexity and dependencies between elements of the structure, especially in the case of global supply networks. On the

other hand, the process approach should be based on the service engineering principles to describe the specificity of the delivery processes (supply, demand and distribution) as accurately as possible. A quantitative description of the system should contain both performance and operability related measures.

Step 6 System designing

Designing complex engineered system for the risky environment is a comprehensive process including two main stages, namely creating reliable system's infrastructure and assurance process continuity. In case of logistics networks architecting reliable engineered system of systems can be based on the principle of High Reliability Organisations, whereas the process continuity ensuring is usually based on the concept of Resilient Enterprise. A detailed describing of the system designing process can be found in Chap. 4—Sects. 4.1 and 4.2.

Step 7 System modelling

Modelling of logistics networks is divided into four main stages: modelling of logistic infrastructures using an agent based approach, modelling of logistic processes applying a dynamic based approach, modelling of demand variation using a probabilistic approach, and modelling of disturbances with an event driven approach. All these processes are described in Chap. 5.

Step 8 Simulation tests

The developed and verified model in step 7 is the starting point for the application phase, which consists in conducting simulation tests. The basis for simulation procedures is provided in Sect. 5.1, while specific solutions for logistics networks are presented in Sects. 5.2–5.5.

Step 9 Operational risk and dependability evaluation

The evaluation of operational risk and dependability for complex engineered systems is a process that can be represented in the form of the general algorithm presented in Fig. 4.6. The method is implemented in 10 stages. The final stage of the proposed procedure is to assess the overall risk matrix, taking into consideration all potential risky scenarios as a consequence of the possible disruptive events. The entire disruption risk matrix will be expressed as a N -dimensional vector, where N is the number of investigated scenarios. The dependability measure of the system under consideration can be expressed by formula (4.3) interpreted as the likelihood to avoid disruptions that are more probable and more severe in consequences than it is acceptable for each possible risky scenario.

Step 10 Acceptance decision

The basis for making a decision about accepting or rejecting the solution are the results obtained in step 9. If the level of operational risk and dependability measure (determined as a result of simulation tests) are acceptable, it can be assumed that the logistics network is sufficiently well protected from threats and hazards. If,

however, the test results are not satisfactory, then you should go back to step 6 and make changes to the system design, and then perform further research (steps 7–10) for the changed configuration of the logistics network. This procedure should be repeated until we receive fully satisfactory results.

6.2 Application Examples of the ELNORD Framework

6.2.1 *A Risk Oriented Static Approach—A Modified PFMEA Method*

Modern organisations are developing frameworks for enterprise risk management (ERM) in response to an increasingly unpredictable global business environment. It allows companies to take corporate risk management in order to actively anticipate, track and manage customer and supplier risks. More and more companies are turning to predictive methods to gain a better and more complete view of long, complex supply chain and distribution networks. Risk at any point on the supply chain becomes the risk at every point, so it's not enough just to focus on the internal threats facing one enterprise, but we have to handle vulnerabilities among each supplier and distributor—and also in the markets of our consumers. The biggest problem is related to integrating and consolidating risk management throughout complex global supply chains and assessing individual suppliers, manufacturers, distributors, vendors and consumers in a more and more complicated logistical environment.

Professional literature devoted a great deal of attention to the problems of suppliers evaluation and selection (Boran et al. 2009; Bross and Zhao 2004; Chen-Tung and Ching-Torng 2006; Chuan 2009; De Boer et al. 1998; Degraeve et al. 2000; Degraeve and Roodhofs 1999; Dulmin and Mininno 2003; Gonzales et al. 2004; Ho et al. 2010; Humphreys et al. 2003; Kuo et al. 2010; Lee et al. 2001; Li et al. 1997; Liu and Hai 2005; Min 1994; Saaty and Vargas 2006; Sanayei et al. 2008; Sharland et al. 2003; Svensson 2004; Tahriri et al. 2008; Weber and Ellram 1992; Welborn 2010), as well as the choice of vendors (Elanchezhian et al. 2010; Faez et al. 2009; Hinkle et al. 1969; Maggie and Tummala 2001; Shyur and Shih 2006; Weber et al. 1991, 1998). Some of these works use artificial intelligence methods such as fuzzy reasoning and artificial neural networks to support decision-making (Boran et al. 2009; Chen-Tung and Ching-Torng 2006; Dong 2007; Faez et al. 2009; Kuo et al. 2010; Saaty and Vargas 2006; Torfi et al. 2010). On the other hand, relatively little attention is paid to the problem of risk on a holistic basis, namely the risk of ensuring the continuity of the product's flow across whole supply chains and networks (Bukowski et al. 2015). Quality standards ISO 9000:2015 and ISO 9001:2015 recommend to use the concept of risk-based thinking for "... carrying out preventive action to eliminate potential nonconformities, analysing any nonconformities that do occur, and taking action to prevent

recurrence that is appropriate for the effects of the nonconformity ...”. To conform to these requirements each organization needs to plan and implement actions to address all possible risks and opportunities, to “... establish a basis for increasing the effectiveness of the quality management system, achieving improved results and preventing negative effects ...”.

Based on this concept the new edition of the Automotive Quality Management System Standard—IATF 16949 (IATF 2016) introduces a requirement that each organization shall have a documented supplier selection process, which shall include “... an assessment of the selected supplier’s risk to product conformity and uninterrupted supply of the organization’s product to their customers ...”, as well as “... organizations shall ensure conformance of all products and processes, including service parts and those that are outsourced ...”. Therefore, each organization is ultimately responsible for all conformity and must cascade all applicable requirements down the whole supply chain, which requires the use of special methods, such as capturing and analysing risk via an FMEA (Failure Mode and Effect Analysis) (Dong 2007; Geum et al. 2011; Guidelines 2017; Welborn 2010).

The aim of this example is to propose a universal method of supply risk assessment, based on expert knowledge and the modified PFMEA (Process Failure Mode and Effect Analysis) methodology. The most important difference between this concept and existing solutions is that the uncertainty of the risk assessment is taken into account, with the use of possibility measures and fuzzy reasoning. The advantage of this approach is the ability to make decisions about the future with the uncertainty awareness of the obtained analytical evaluation.

6.2.1.1 Supplier Selection Methods

The basic criteria typically utilized for supplier selection are: costs, delivery time, product quality, and service level. Traditionally most buyers consider cost as the primary decision factor, but recently more and more various criteria for the supplier selection are taken into account: performance history, warranties and claims policies, production facilities and capacity, financial position, procedural compliance, reputation and position in industry, desire for business, repair service, attitude, packaging ability, geographical location, amount of past business, and reciprocal arrangement. With economic globalization, companies can choose suppliers from anywhere in the world, and developing countries are becoming more competitive because of their low labour and operating costs.

Different supplier selection methods observed in the literature can be classified as follows:

- **Categorical Methods (CM).** CM are qualitative models; based on historical data and experience, current suppliers are evaluated on a set of criteria. The primary advantage of the categorical approach is that the evaluation process is easy, clear and systematic.

- **Data Envelopment Analysis (DEA).** DEA is a classification system that splits suppliers between two categories, namely ‘efficient’ or ‘inefficient’. Suppliers are judged on two sets of criteria, i.e. outputs and inputs. Weber et al. have discussed the application of DEA in supplier selection in several publications (e.g. Weber et al. 1998).
- **Cluster Analysis (CA).** CA is a method based on statistics which uses a classification algorithm to group a number of items described by a set of numerical attribute scores into a number of clusters. This classification is used to reduce a larger set of suppliers into smaller more manageable subsets (Hinkle et al. 1969).
- **Analytical Hierarchical Process (AHP).** AHP is a decision-making method developed for prioritizing alternatives when multiple criteria have to be considered and allows the decision maker to structure complex problems in the form of a hierarchy. This method incorporates qualitative and quantitative criteria. The hierarchy usually consists of three different levels, which include goals, criteria, and alternatives. Because AHP utilizes a ratio scale for human judgments, the alternative weights reflect the relative importance of the criteria in achieving the goal of the hierarchy (Hill et al. 1992; Maggie and Tummala 2001; Sharland et al. 2003).
- **Analytic Network Process (ANP).** ANP is a comprehensive decision-making technique that captures the outcome of the dependence and feedback within and between the clusters of elements. ANP is more general than AHP, incorporating feedback and interdependent relationships among decision attributes and alternatives. ANP is a coupling of two parts, where the first consists of a control hierarchy or network of criteria and subcriteria that controls the interactions, while the second part is a network of influences among the elements and clusters (Saaty and Vargas 2006).
- **Total Cost of Ownership (TCO).** TCO-based models for supplier choice consist of summarization and quantification of several costs associated with the choice of vendors and subsequently adjusting or penalizing the unit price quoted by the supplier. TCO is a methodology and philosophy, which looks beyond the price of a purchase to include many other purchase-related costs (Pearson and Ellram 1995).
- **Technique for the Order Performance by Similarity to Ideal Solution (TOPSIS).** Consistent with the concept of the TOPSIS, a closeness coefficient is defined to determine the ranking order of all suppliers and linguistic values are used to assess the ratings and weights of the factors. TOPSIS is based on the concept that the optimal alternative should have the shortest distance from the positive ideal solution (PIS) and the farthest distance from the negative ideal solution (NIS) (Sharland et al. 2003).
- **Multiple Attribute Utility Theory (MAUT).** The MAUT proposed by Min (1994) is considered a linear weighting technique. The MAUT method has the advantage that it enables purchasing professionals to formulate feasible sourcing strategies and is capable of handling multiple conflicting attributes. However,

this method is mostly used for international supplier selection, where the environment is more complicated and risky (Svensson 2004).

- **Outranking Methods (OM).** OM are useful decision tools to solve multi-criteria problems. These methods are capable of dealing with situations in which imprecision is present. Lot of attention has been paid to outranking models, however, so far, in the literature there is no evidence of applications of outranking models in purchasing decisions.
- **Mathematical programming models (MPM).** MPM often consider only the quantitative criteria. Mathematical programming models allow decision makers to consider different constraints in selecting the best set of suppliers. MPM are particularly useful for solving the supplier selection problem because they can optimize results using either single objective models or multiple objective models (Chen-Tung and Ching-Toring 2006; Weber et al. 1992).
- **Case-Based-Reasoning (CBR).** CBR systems fall in the category of the artificial intelligence (AI) approach. Basically, a CBR system is a software-driven database which provides a decision-maker with useful information and experiences from similar, previous decision situations. CBR is still very new and only few systems have been developed for purchasing decision making (Kuo et al. 2010).
- **Artificial Neural Network (ANN).** The ANN models are very efficient when we have access to a large number of credible data. The weakness of this model is that it demands specialized software and requires highly-qualified experts (Kuo et al. 2010).
- **Fuzzy logic approach (FLA).** In this method, linguistic values are used to assess the ratings and weights for various factors and criteria. Usually these linguistic ratings can be expressed in trapezoidal or triangular fuzzy numbers. (Boran et al. 2009; Chen-Tung and Ching-Toring 2006; Faez et al. 2009; Torfi et al. 2010).
- **Hybrid methods (HM).** Some authors have combined different decision models into a supplier selection process. Degraeve and Roodhooft (1999) developed a model combining Mathematical Programming Model with Total Cost of Ownership methodology. Ghodsupour and O'Brien (1998) had integrated AHP and Linear Programming to consider both tangible and intangible factors in choosing the best suppliers. Sanayei et al. (2008) presented an effective model using both MAUT and LP for solving the supplier selection problem. Boran et al. (2009) has proposed a multi-criteria group decision making approach using fuzzy TOPSIS, to deal with uncertainty.

None of the above methods meet the requirements of the IATF 16949 regarding risk-based thinking. Thus, there is a need to develop a new method, which is focused on “an assessment of the selected supplier’s risk to product conformity and uninterrupted supply of the organization’s product to their customers”.

6.2.1.2 Risk Assessment Methodology—Process Failure Mode and Effects Analysis

Process Failure Mode and Effects Analysis (PFMEA) is a methodical approach used for identifying risks related to process changes, and focused on potential process failures and their causes. The PFMEA initially identifies process functions, failure modes, their effects on the process and the effect on end user. The consequence of the effect is determined for each effect of failure. Then, causes and their mechanisms of the failure mode are identified. Based on the Appendix E of the AIAG, Potential Failure Mode and Effects Analysis (FMEA) 4th Edition (AIAG 2008), the basic concepts used in PFMEA are defined in the following way:

Function (FU)—the objective which the process is intended to do, to a given standard of performance or requirement. For Process FMEAs, this is the primary purpose of the delivering, manufacturing or assembly operation. There may be many functions for each operation.

Failure (FA)—the state or condition of inability to perform a required function.

Failure Cause (FC)—the specific reason for the failure. For PFMEAs, the cause is the process deficiency (or source of variation) that results in the failure mode; if a cause occurs, the corresponding failure mode occurs. There can be many causes for each failure mode.

Failure Mode (FM)—the manner in which the item or operation fails to meet or deliver the intended function and its requirements. Failure modes may include failure to perform a function within defined limits, inadequate or poor performance of the function, intermittent performance of a function, and/or performing an unintended or undesired function. There may be many failure modes for each function.

Failure Effect (FE)—the consequence of the failure on the system or end user. For PFMEAs, usually we consider the effect of the failure at the delivering, manufacturing or assembly level, as well as at the system or end user. There can be more than one effect for each failure mode, but generally we use the most serious of the end effects for the analysis.

Process Controls (PC)—the methods or actions to reduce or eliminate the risk associated with each potential cause. Controls can be the methods to prevent or detect the cause during product development, or actions to detect a problem during service before it becomes disastrous. There can be many controls for each cause.

Prevention related Process Controls (PPC)—the methods that describe how a cause, failure mode, or effect in the delivering, manufacturing or assembly process is prevented. They are intended to reduce the likelihood that the problem will occur, and are used as input to the occurrence ranking.

Detection related Process Controls (DPC)—the methods that describe how a failure mode or cause in the delivering, manufacturing or assembly process is detected. They are intended to increase the likelihood that the problem will be detected before the item is shipped from the manufacturing or assembly plant, and are used as an input to the detection ranking.

Corrective Actions (CA)—the tasks that can be performed to reduce or eliminate the risk associated with potential cause of failure. Corrective actions should consider the existing controls, the relative importance of the issue, and the cost and effectiveness of the recommended action. There can be many types of actions for each cause.

Ranking Numbers (RN)—usually integer numbers ranging from 1 to 10.

Severity(S)—a ranking number associated with the most serious effect for a given failure mode based on the criteria from a severity scale. It is a relative ranking within the scope of the specific PFMEA and is determined without regard to the likelihood of occurrence or detection.

Occurrence (O)—a ranking number associated with the likelihood that the failure mode and its associated cause will be present in the item being analysed. For PFMEAs the occurrence ranking considers the likelihood of occurrence during delivering or production process. It is based on the criteria from the corresponding occurrence scale. The occurrence ranking has a relative meaning rather than an absolute value and is determined without regard to the severity or likelihood of detection.

Detection (D)—a ranking number associated with the best control from the list of detection-type controls, based on the criteria from the detection scale. The detection ranking considers the likelihood of detection of the failure mode/cause, according to defined criteria. Detection is a relative ranking within the scope of the specific PFMEA and is determined without regard to the severity or likelihood of occurrence.

Risk Priority Number (RPN)—is a numerical ranking (usually integer numbers ranging from 1 to 1000) of the risk of each potential failure mode/cause, made up of the three elements product: severity of the effect, likelihood of failure mode occurrence/cause, and likelihood of detection of the failure mode/cause.

Once the expert team have completed the initial identification of failure causes, failure modes and failure effects, as well as process controls, including rankings for severity, occurrence and detection, they have to decide if further efforts are needed to reduce the risk. The main focus of the expert team should be oriented towards failure modes with highest severity rankings. When the severity rank is 9 or 10, they must ensure that the risk is mitigated by process controls or recommended corrective actions. For failure modes with severity ranks 8 or below the expert team should consider causes having highest occurrence rank, and next detection ranking. If occurrence rate is greater than 8, then action(s) is initiated in order to reduce the likelihood of failure mode occurrence (Guidelines 2017).

6.2.1.3 Modified Process Failure Mode and Effects Analysis for Supply Risk Assessment

The supply risk assessment procedure is a process that can be divided into the following 14 steps:

- (1) Review the process using a flowchart to identify each process component.
- (2) Setting of acceptable risk level as target risk priority number (TRPN).
- (3) Brainstorm potential failure modes (FM) and failure causes (FC) reviewing existing documentation and historical data.
- (4) List potential effects of failure (FE) (usually more than one for each failure).
- (5) Assign the Severity (S) rankings for each failure mode based on the criteria from Table 6.1.
- (6) Assign failure causes occurrence for each failure mode (CO) based on Table 6.2.
- (7) Assign effectiveness of the prevention related process controls (EP) in scale from 0 to 1.
- (8) Calculate the Occurrence (O) rankings for each failure mode based on how frequently the failure mode is likely to occur despite preventive actions as a product: $O = CO \times (1 - EP)$.
- (9) Assign Detection (D) rankings for each failure mode based on the chances the failure will be detected as in Table 6.3.
- (10) Calculate the Risk Priority Number (RPN) as product of Severity, Occurrence and Detection: $RPN = S \times O \times D$ as fuzzy number and its defuzzification to crisp number.
- (11) Compare the calculated RPN value with the target value of TRPN.
- (12) Develop the Corrective Actions (CA) plan for failure modes with $RPN > TRPN$.
- (13) Implement the improvement actions.

Table 6.1 Severity rating scale

Rating	Description	Severity of failure effect
10	Dangerously high	Failure could highly affect the supplier and customers
9	Extremely high	Failure would create noncompliance with standards or regulations
8	Very high	Failure renders the unit inoperable or unfit for use
7	High	Failure causes a high degree of customer dissatisfaction
6	Moderate	Failure results in partial malfunction of the supply
5	Low	Failure creates enough of a performance loss to cause the customer to complain
4	Very low	Failure causes a minor performance loss, and can be overcome with supplier process modifications
3	Minor	Failure creates a minor nuisance to the supplier, but it can be removed without performance loss
2	Very minor	Failure may not be visible to the supplier, but would have minor effects on the supply process
1	None	Failure would not be noticeable to the supplier and would not affect the supplier process

Table 6.2 Occurrence rating scale

Rating	Description	Potential failure rate
10	Very high (almost inevitable)	More than 1 occurrence per day or probability of more than 3 in 10 events
9	High (very often)	1 occurrence every 3 to 4 days or a probability of 3 in 10 events
8	High (repeated failures)	1 occurrence per week or a probability of 5 occurrences in 100 events
7	High (often)	1 occurrence every month or one occurrence in 100 events
6	Moderately high (frequent)	1 occurrence every 3 months or 3 occurrences in 1000 events
5	Moderate (occasional)	1 occurrence every 6 months to 1 year or 5 occurrences in 10,000 events
4	Moderately low (infrequent)	1 occurrence per year or 6 occurrences in 100,000 events
3	Low (relatively few)	1 occurrence every 1 to 3 years or 6 occurrences in 10 million events
2	Low (few and far between)	1 occurrence every 3 to 5 years or 2 occurrences in one billion events
1	Remote (unlikely)	1 occurrence in greater than 5 years or less than 2 in one billion events

Table 6.3 Detection rating scale

Rating	Description	Likelihood of the failure mode detection
10	Absolute uncertainty	Failure is undetectable and uncontrollable
9	Very remote	Failure can be detected only with thorough inspection and this is uncontrollable
8	Remote	Failure is detected based on no effects in a events
7	Very low	Failure can be detected with manual inspection but detection is left to chance
6	Low	Failure is fully manually detected using mistake-proofing techniques
5	Moderate	Failure is partially detected and partially controlled
4	Moderately high	Failure is partially detected and it is control conditions
3	High	There is full detection or total review of the process but it is not automated
2	Very high	All failures are automatically detected
1	Almost certain	Failure is obvious or there is full automatic detection and it is easy to take a preventive action

- (14) Calculate the residual risk priority number (RRPN) evaluating the impact of the improvements.

The method has been verified on the example of a real supply chain. Due to the lack of statistical data on the occurrence of failures and their possible effects in the past, we used the expert knowledge to set up potential failure modes (FM), failure causes (FC), failure effects (FE), process controls (PC), corrective actions (CA) and RPN target limits, as well as for the evaluation of numerical indicators X_i , e.g. $S(FM_j)$, $CO(FM_j)$, $EP(FM_j)$ and $D(FM_j)$. The team of three experts evaluated each of the above parameters by the three numbers corresponding to the minimum value, the most likely value and the maximum value of the indicators. These numbers were the basis for describing a *uncertainty measures* as triangular membership function of a variable X in terms of the fuzzy sets theory. The results of the evaluation are therefore triangular membership functions in a number equal to the amount of the experts involved in the assessment process (Bukowski and Feliks 2005). Aggregation of expert assessments can be done by building a collective triangular membership function with the parameters:

$$X_i = f(x_i - a_i; x_{im}; x_i + b_i), \text{ for } i = 1 \dots n \quad (6.1)$$

where: $x_{im} = 0,5(x_{imin} + x_{imax})$ and the parameters a and b are calculated from the Hartley's formula (Hartley 1928) as a function of two standard deviations of the all three experts evaluations (which corresponds to a confidence interval for x of around 95%).

Potential failures modes (FM_j) were divided into three groups, each consisting of two elements:

Quality—compliance deviation (FM1)

- product/service incorrectness (FM1a)
- incomplete delivery (FM1b)

Costs—nonconformity (FM2)

- increased unit price (FM2a)
- increased transportation costs (FM2b)

Lead time—tardiness (FM3)

- delay of delivery (FM3a)
- too early delivery (FM3b)

The results of the investigation for one of the suppliers (supplier X) are shown in Table 6.4. The graphic interpretation of these assessments for 'the worst case' (FM3a—failure modes 'delay of delivery') is presented in Figs. 6.2 and 6.3. The criteria for FM3a and FM3b were not met, so a corrective action plan was proposed. *Redundancy and stocks* have been recognized as prevention related Process Controls (PPC), and the *traceability* as detection related Process Controls (DPC). As a result of these actions, the RRPN values were reduced to the level below

Table 6.4 (continued)

FM	EVAL	S	CO	EP	O	D	RPN	CA	S _c	O _c	D _c	RRPN
FM2b	EXP.A	2, 3, 4	5, 6, 7	0.1, 0.2, 0.3	3.5, 4.8, 6.3	1, 2, 4						
	EXP.B	2, 3, 4	6, 7, 8	0.1, 0.2, 0.3	4.2, 5.6, 7.2	1, 2, 4						
	EXP.C	2, 3, 4	4, 6, 8	0.1, 0.2, 0.3	2.8, 4.8, 7.2	1, 2, 4						
	AGGR.	2.1, 3, 3.9	4.4, 6.5, 7.8	0.1, 0.2, 0.3	3.1, 5.2, 6.9	1.2, 2.0, 3.7	42.9	NO				
FM3a	EXP.A	7, 8, 9	6, 7, 8	0.1, 0.2, 0.3	4.2, 5.6, 7.2	7.0, 8.0, 8.99			4, 5, 6	0.3, 0.8, 1.5	7, 8, 9	
	EXP.B	6, 8, 10	7, 8, 9	0.2, 0.3, 0.4	4.2, 5.6, 7.2	4.0, 5.0, 7.99			3, 5, 6	0.8, 1.5, 2.4	4, 5, 8	
	EXP.C	8, 9, 10	7, 8, 10	0.2, 0.5, 0.6	2.8, 4.0, 7.9	6.0, 7.0, 7.99			4, 5, 6	0.4, 1.2, 2.1	6, 7, 8	
	AGGR.	6.4, 8.5, 9.8	6.2, 7.5, 9.6	0.1, 0.3, 0.5	2.7, 4.8, 8.3	4.38, 6.50, 8.62	329.5	YES	3.3, 5.0, 5.8	0.4, 1.3, 2.5	4.4, 6.5, 8.6	53.3
FM3b	EXP.A	4, 5, 6	3, 4, 5	0.1, 0.2, 0.3	2.1, 3.2, 4.5	4, 6, 8			4, 5, 6	0.9, 1.6, 2.5	4, 6, 8	
	EXP.B	4, 6, 7	4, 5, 6	0.2, 0.4, 0.6	1.6, 3.0, 4.8	6, 7, 8			4, 6, 7	0.8, 2.0, 3.6	6, 7, 8	
	EXP.C	3, 5, 7	4, 6, 7	0.2, 0.3, 0.4	2.4, 4.2, 5.6	7, 8, 9			3, 5, 7	0.4, 1.2, 2.0	7, 8, 9	
	AGGR.	3.4, 5.5, 6.8	3.3, 5.0, 6.7	0.1, 0.3, 0.5	1.5, 3.5, 5.8	4.5, 7.0, 8.7	154.9	YES	3.4, 5.5, 6.8	0.4, 1.5, 3.7	4.5, 7.0, 8.7	85.9

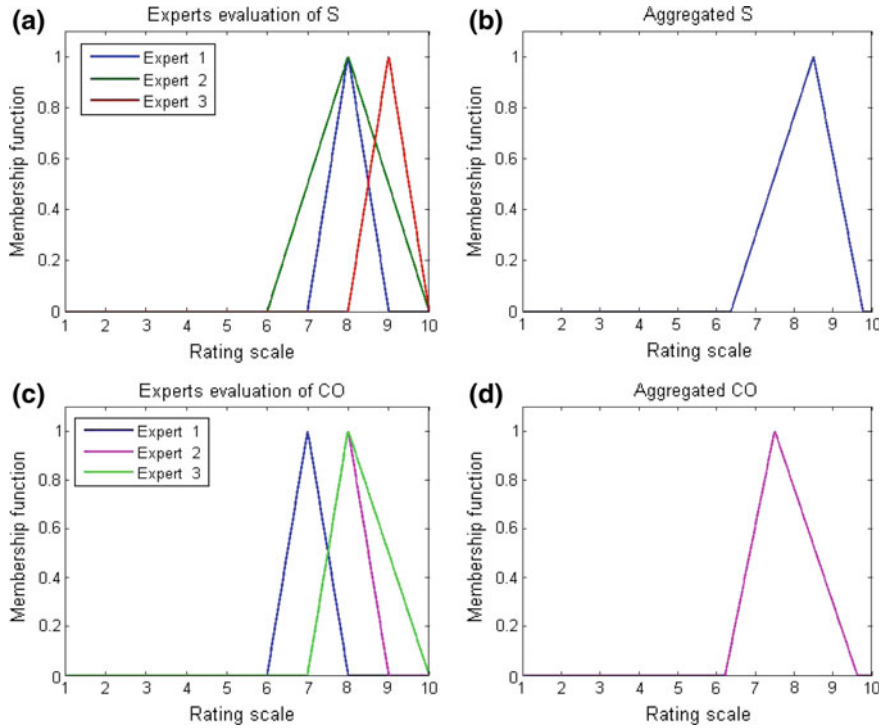


Fig. 6.2 The graphic interpretation of the supply risk assessments for supplier X with regard to failure mode FM3a: **a** experts evaluation of S; **b** experts evaluation of S after aggregation; **c** experts evaluation of CO; **d** experts evaluation of CO after aggregation

TRPN = 100, so it was assumed that the analysed supplier meets the requirements to a sufficient degree.

6.2.1.4 Conclusions

Organizations need to plan and implement actions to address all possible risks and opportunities as well as to establish a basis for improving their results and preventing negative effects. One of the biggest problems in achieving this goal is related to integrating and consolidating risk management throughout complex global supply chains and assessing individual suppliers, manufacturers, distributors, vendors and consumers in a complicated logistical environment. In the paper we propose a universal method of supply risk assessment, based on expert knowledge and the modified Process Failure Mode and Effect Analysis methodology. The most important difference between this concept and existing solutions is, that the uncertainty of the risk assessment is taken into account, with the use of possibility measures and fuzzy reasoning.

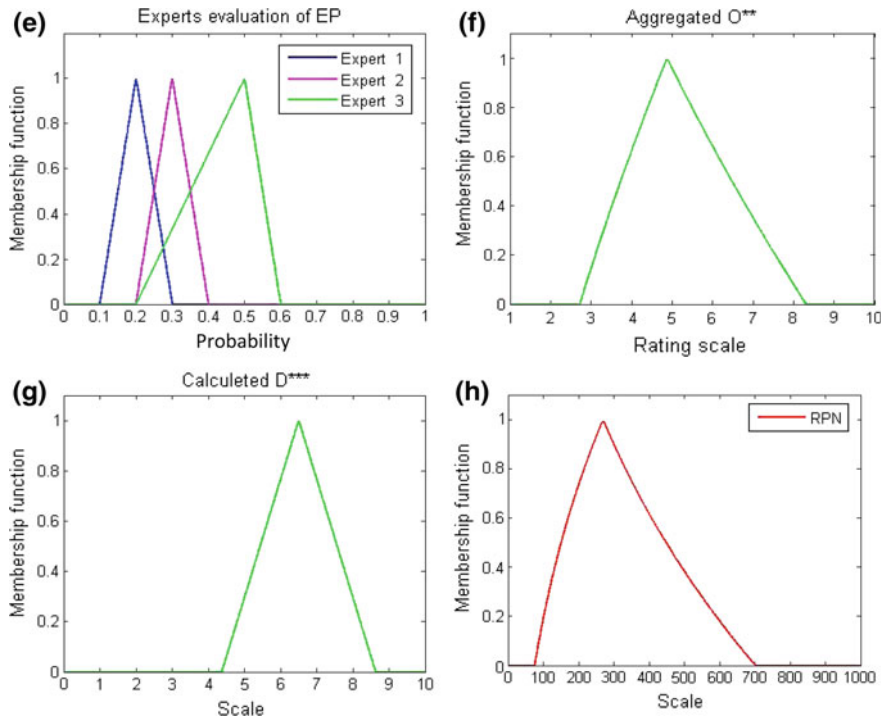


Fig. 6.3 The graphic interpretation of the supply risk assessments for supplier X with regard to failure mode FM3a: **e** experts evaluation of EP; **f** evaluation result of O after aggregation and multiplication; **g** experts evaluation of D after aggregation; **h** RPN as a fuzzy number

The method has been verified on the example of a real supply chain. Due to the lack of statistical data on the occurrence of failures and their possible effects in the past, we used the expert knowledge to set up potential failure modes (FM), failure causes (FC), failure effects (FE), process controls (PC), corrective actions (CA) and RPN target limits, as well as for the evaluation of numerical indicators $S(FM_j)$, $CO(FM_j)$, $EP(FM_j)$ and $D(FM_j)$. The team of the experts evaluated each of the above parameters by the three numbers corresponding to the minimum value, the most likely value and the maximum value of the indicators. These numbers were the basis for describing uncertainty measures as triangular membership functions of a variable X in terms of the fuzzy sets theory. The results of the evaluation are therefore triangular membership functions in a number equal to the amount of the experts involved in the assessment process. Potential failure modes were divided into three groups (quality, costs and lead time), each consisting of two elements. Where these criteria were not met, a corrective action plan was proposed. If as a result of these actions the RPN values were reduced to the level below TRPN, it was assumed that the analysed supplier meets the requirements to a sufficient degree. In order to select the best suppliers fulfilling this condition, the calculated

RPN (or RRPN) values for each FM were multiplied by the respective weights, and then the values obtained together were summed up. The best supplier was the one with the smallest sum of points.

6.2.2 A Process Continuity Oriented Approach—An Expert System with Fuzzy Reasoning for Disruption Risk Prediction in Logistics Networks

The object of our interest in this example is the operational risk occurring in the large scale complex systems, such as global supply chains. One of the major operational problems in these systems is risk of loss of business continuity. We define the continuity as a system capability to deliver products and/or services at acceptable predefined performance level under the real work conditions. The continuity can be interrupted by disruptive events, such as system failures, natural catastrophes and man-made faults. This type of risk is called disruption risk. Based on Sect. 2.3 and taking into account the current possibilities of modelling uncertainty, we understand *disruption risk* as a potential for realization of unwanted scenario leading to a disruptive event with possibility of negative consequences.

6.2.2.1 A Framework for Disruption Risk Evaluation of a Logistics Network

The objective of this example is to apply the general framework for Evaluation of Logistic Networks Operational Risk and Dependability (ELNORD) for quantitative risk assessment related to the occurrence of different threats and hazards, and resulting in disrupting process continuity on a large scale. This problem is particularly important for large scale complex systems, for instance, the global supply networks.

The disruption risk evaluation of a whole investigated complex system is a process that can be represented in the form of the algorithm shown in Fig. 6.4 (based on the general algorithm presented in Fig. 4.8). The method is implemented in seven steps. Firstly, a team of experts selects potential sources of risk $\{RS_i\}$, based on the literature, data and their own experience. The collection of $\{RS_i\}$ is the basis for generating a set of possible threats and hazards creating risky scenarios $\{TH_j\}$, which actually may occur within the analysed system. Then Experts estimate the probability of occurrence of each of these scenarios $\{P(TH_j)\}$. A properly designed complex system, especially large scale network, should be equipped with a security subsystem consisting of a number of proactive barriers $\{PB_k\}$, which are designed to prevent direct exposure of the system to a loss of its ability to perform the function. Thus, the next step is to assess the effectiveness of barriers in case of each of the potential threats and hazards as a probability of preventing the system exposure $\{P(PB_k)\}$.

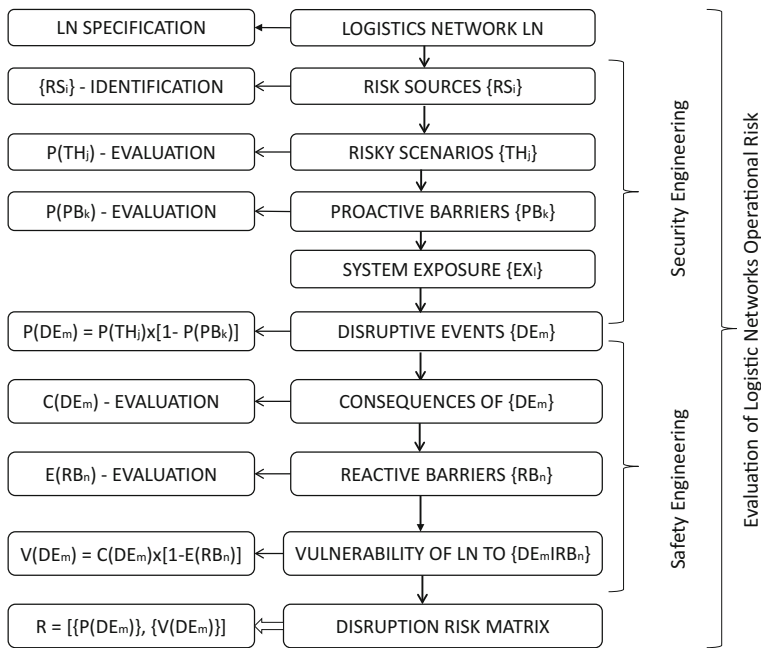


Fig. 6.4 The algorithm for disruption risk evaluation of a logistics network

These risks, which are not effectively blocked by security barriers, become direct system exposures $\{EX_i\}$ and are defined as the initiating events that can interrupt the continuity of process $\{DE_m\}$ (disruptive events). To these events we should prescribe the measures of uncertainty of their occurrence, e.g. in the form of probabilities $\{P(DE_m)\}$. The next stage of the process is a comprehensive evaluation of resilience of the system to the exposure (we understand the term resilience as the ability of a system to absorb and withstand the disruption impact, and still continue to deliver products and/or services at acceptable predefined performance level), the estimation of the susceptibility of the analysed system to individual exposure and the prediction of the effects of events $\{DE_m\}$ in the form of losses caused by these events $\{C(DE_m)\}$ (consequences). The next step is to assess the efficacy of reactive barriers $\{E(RB_n)\}$ (safety subsystem), which are designed to protect the complex system and its environment against the effects of disruptive events. Then, we can evaluate the vulnerability of the entire complex system to the particular disruptive events $\{V(DE_m)\}$.

The final step of the proposed procedure is to assess the overall risk of a disruption, taking into consideration all possible scenarios and their consequences $\{C_i\}$. The entire disruption risk will be expressed as an m -dimensional vector $R = [\{P(DE_m)\}, \{V(DE_m)\}]$, where m is the number of a possible disruptive scenarios.

6.2.2.2 Implementation Example of the Framework

The usefulness of the method presented in Sect. 6.2.1.1 has been verified on the example of a global scale logistics network (LN). Due to the lack of statistical data on the occurrence of past threats, destructive events and their possible consequences, we used the expert knowledge for the evaluation of numerical indicators X_i —e.g. $P(\cdot)$, $C(\cdot)$ and $E(\cdot)$. The team of three technical experts evaluated each of the above parameters by the three numbers corresponding to the maximum value, the most likely value and the minimum value of the indicators. These numbers were the basis for describing a triangular membership function of a random variable X in terms of the fuzzy sets theory.

The results of the evaluation are therefore triangular membership functions in a number equal to the amount of the experts involved in the assessment process (in this example three). Aggregation of expert assessments can be done by building a collective triangular membership function with the parameters a and b (see formula 6.1) which are calculated from the Hartley’s formula (Hartley 1928) as a function of the standard deviation of the all three experts evaluations. In our example we assume that both these parameters represent a value of two standard deviations.

Step 1 Risk sources identification

The team of three experts selected potential sources of risk $\{RS_i\}$, based on the literature, data and their own experience. The set $\{RS_i\}$ was the basis for generating a set of six most dangerous scenarios of the threats and hazards $\{TH_j\}$, which potentially may occur within the analysed system.

Step 2 Evaluation of threats and hazards probabilities

The probability of occurrence for each of the risks was assessed by each of the three experts. Table 6.5 shows an example of the threat likelihood assessment for scenario S_1 .

The graphic interpretation of these assessments is presented in Fig. 6.5a, and the result of aggregation of all three expert evaluations is shown in Fig. 6.5b. The parameters of the function $P(TH_1)$ after aggregation are [0.193, 0.375, 0.609].

Step 3 Evaluation of proactive barriers effectiveness

The next step is to assess the effectiveness of the security barriers in the case of each of the potential threats and hazards. The effectiveness of this proactive barriers $\{PB_k\}$ was defined as a probability of preventing the direct exposure of the system

Table 6.5 An example of the threat likelihood assessment for scenario S_1

	$P(TH_{1min})$	$P(TH_{1m})$	$P(TH_{1max})$
Expert 1	0.2	0.3	0.4
Expert 2	0.3	0.4	0.5
Expert 3	0.2	0.45	0.6

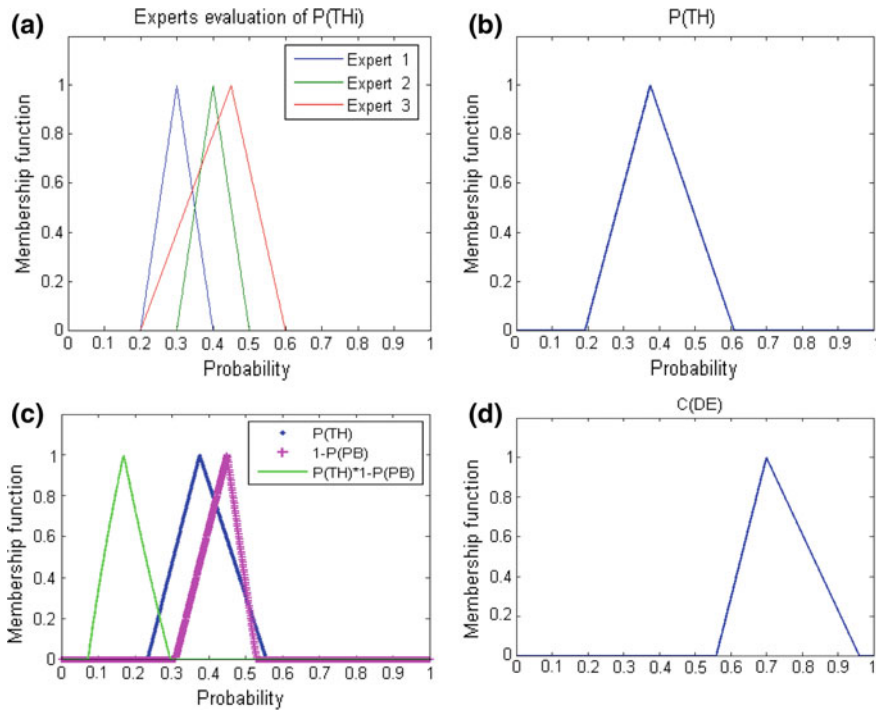


Fig. 6.5 The graphic interpretation of the threat likelihood assessment for scenario S_1 : **a** experts evaluation of $P(TH_i)$; **b** experts evaluation of $P(TH_i)$ after aggregation; **c** evaluation of the function $P(DE_i)$; **d** experts evaluation of $C(DE_i)$ after aggregation

to a loss of its ability to perform the function. For this purpose, the same evaluation procedure as in Step 2 was used. After the aggregation of the results of individual experts evaluations for scenario S_1 we received the function with parameters $P(PB_1) = [0.41, 0.55, 0.69]$.

Step 4 Evaluation of disruptive events probabilities and consequences

This procedure step involves the determination of the probability of an event that could not be 'stopped' with the barrier. We get it by multiplying the aggregate triangular membership functions according to the formula

$$P(DE_m) = P(TH_j) * [1 - P(PB_k)] \quad (6.2)$$

Multiplication effect is shown in Fig. 6.5c, and the parameters of the resulting triangular function $P(DE_i)$ for the data presented above are $[0.07, 0.17, 0.3]$. The next stage of the process involves the evaluation of robustness and resilience of the system to given exposure, the estimation of the susceptibility of the analysed system to individual exposure and the prediction of the effects of events $\{DE_m\}$ in the form of consequences caused by these events $\{C(DE_m)\}$. As a measure of the

parameter $C(DE_m)$ we have chosen the relative value of the expected loss given a disruptive event in a system. The function $C(DE_1)$ for scenario 1 after aggregation is shown in Fig. 6.5d.

Step 5 Evaluation of reactive barriers efficacy

The next step is to assess the efficacy of reactive barriers $\{E(RB_n)\}$ in safety subsystem, which is designed to protect the complex system and its environment against the effects of disruptive events. The efficacy of the reactive barriers $\{RB_n\}$ was defined as a probability of protecting the complex system and its environment against the effects of disruptive events. Experts agreed that in scenario S_1 there are no efficient reactive barriers, so $E(RB_1) = 0$.

Step 6 Evaluation of the complex system vulnerability

In this step we have to evaluate the vulnerability of the entire complex system to the particular disruptive events $\{V(DE_m)\}$ based on the general formula:

$$V(DE_m) = C(DE_m) * [1 - E(RB_n)] \quad (6.3)$$

The vulnerability metric was defined as the relative value of the expected loss given a disruptive event in a system. Since in the case of scenario S_1 efficacy of the reactive barrier is 0, vulnerability $V(DE_1)$ is equal consequences $C(DE_1)$. Figure 6.6e shows a graphical interpretation of $P(DE_1)$ and $V(DE_1)$ for the scenario S_1 .

Step 7 Disruption risk matrix assessment

As a result of the six steps we received fuzzy values of probabilities and vulnerabilities for all analysed scenarios of potential threats. To build a risk matrix we must convert the fuzzy values to crisp numbers. These calculations were carried out by the centre of gravity method with the use of Matlab[®] software. Table 6.6 shows the results of calculations for the six most likely scenarios.

As a practical measure of risk we have chosen the product of disruption event probability and vulnerability of the system to this disruption event, for each of the possible scenarios:

$$R(S_i) = P(DE_i) * V(DE_i) \quad (6.4)$$

In case of the analysed systems, the maximum acceptable risk value was set at 0.1 (10%). The only scenario which does not meet this requirement is the scenario S_1 . Therefore, it was decided to modify the system by designing additional reactive barrier, which effectively reduce system vulnerability to the disruptive event DE_1 . After the modifications the recalculations have been made for scenario S_1 in terms of steps 5, 6 and 7. Table 6.7 shows the reactive barrier effectiveness assessment for the modified scenario S_{1mod} .

The graphic interpretation of these assessments is presented in Fig. 6.6f and the result of aggregation of all three experts' evaluation is shown in Fig. 6.6g. The vulnerability fuzzy function for the modified scenario S_{1mod} is shown in Fig. 6.6h.

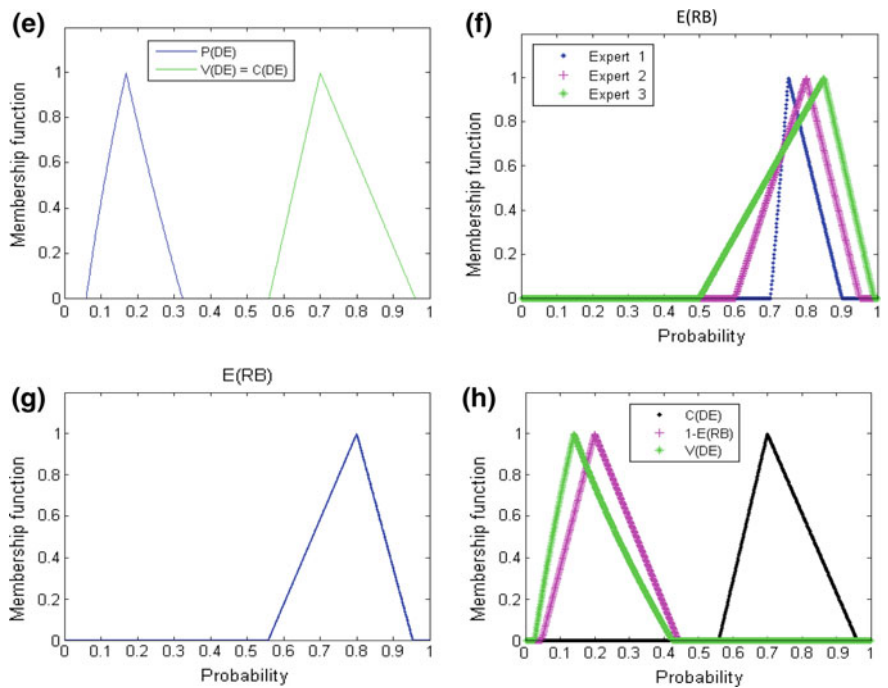


Fig. 6.6 Disruptive event probability and the complex system vulnerability for scenario S_1 : **e** $P(DE_1)$ and $V(DE_1)$ as fuzzy numbers; **f** expert evaluation of modified reactive barriers efficacy; **g** reactive barriers efficacy after aggregation; **h** vulnerability fuzzy function for the modified scenario S_{1mod}

Table 6.6 Disruption risk matrix

Scenario	$P(DE_m)$	$V(DE_i)$	$R(S_i)$
S1	0.180	0.740	0.133
S2	0.269	0.140	0.038
S3	0.373	0.179	0.067
S4	0.412	0.191	0.079
S5	0.512	0.160	0.082
S6	0.821	0.028	0.023

Table 6.7 The reactive barrier efficacy assessment for the modified scenario S_{1mod}

	$E(RB_{min})$	$E(RB_m)$	$E(RB_{max})$
Expert 1	0.7	0.75	0.9
Expert 2	0.6	0.8	0.95
Expert 3	0.5	0.85	0.99

After the converting of fuzzy values to crisp numbers we achieved: $R(S_{1\text{mod}}) = [0.176, 0.190]$ and as the end-result $R(S_{1\text{mod}}) = 0.033$, which was considered as a fully satisfactory result.

6.2.2.3 Conclusions

Disruption risk prediction for large scale complex systems is a process that can be represented in the form of the framework shown in Fig. 6.4. This method can be implemented iteratively, and is divided into seven main steps. The procedure for the disruption risk assessment was based on the assumption of imperfect knowledge about the possible sources of risk, threats and hazards, as well as their consequences for the system. Therefore, we accepted expert evaluation and fuzzy inference as a basis of knowledge.

The usefulness of the presented method has been verified on the example of a global scale logistics network. As a practical measure of risk we have chosen the product of disruption event probability and vulnerability of the system to this disruption event, for each of the possible scenarios. The maximum acceptable risk value was set and the scenarios which do not meet this requirement have been chosen. Therefore, it was decided to modify the system by designing additional reactive barrier, which effectively reduces system vulnerability to the most dangerous disruptive events. This procedure should be iteratively repeated as long as the risk value reaches a satisfactory result for all possible scenarios.

6.2.3 *A Vulnerability Related Dynamic Approach—An Expert System with Agent-Based Simulation*

One of the main problems in modern logistics systems management, especially within the global supply network, is the disruption risk and loss of supply continuity (Security Service 2006; Waters 2007). It results from the efforts to minimize costs by introducing Lean Manufacturing, Lean Logistics, and Lean Management as well as from the increasing number and intensity of external threats. Reducing the number of suppliers according to the “4S” principle (a Single Source Supply Strategy), introducing to a greater extent the Just In Time Manufacturing system, minimizing the level of buffers, and configuring tightly connected supply chains have resulted in a significant increase in the level of delivery disruption risk (Cavinato 2004; Jüttner 2005; Kleindorfer and Saad 2005; Malone 2006; Natarajathinam et al. 2009; Scarborough 2007). Based on these works, as well as on the main trends in the risk understanding (Aven 2014; Aven et al. 2014) we propose the framework for disruption risk modelling in the complex logistic networks.

The objective of this example is to come up with a concept of vulnerability and resilience modelling for the complex logistic systems, and especially the global supply networks ones. The core idea of the overall concept is based on the experiences gained in the area of the supply chain risk management, the service engineering, the reliability engineering as well as that in the field of the resilience engineering. Based on the assumptions of Samson's Unified Service Theory (Sampson 2010), we propose a general model of a complex logistics system, consisting of two parts representing both the inward and the outward logistics (see Sect. 3.2, Fig. 3.4). In the first part of the model there are mapped upstream operations, related to supply of the focus organization in raw materials, necessary to carry out the production. The second part of the model includes downstream operations and also processes corresponding to the distribution of products to the first-tier and second-tier customers.

The model is dynamic and takes into account the possible disruptive events, e.g. disruption in supply process and unforeseen changes in demand. The model structure is based on multi-agent systems (D'Inverno and Luck 2004; Swaminathan, Smith and Sadeh 1998). Implementation of the model has been made on the example of steel mills, whose logistics system is global. Simulation studies on this model were designed to evaluate the resilience of the whole logistics system to disturbances occurring in both its parts.

6.2.3.1 Logistic Networks Vulnerability and Resilience Metrics

Although the ideas of vulnerability and resilience were introduced relatively recently, they have already been examined in many serious studies, both theoretical and practical, in the area of engineered systems (e.g. AMBER 2009; Aven 2011; Dekker et al. 2008; Hollnagel et al. 2006; Kroger and Zio 2011; Sanchis et al. 2012; Sheffi 2007). Also in the area of logistics and supply chains a significant number of interesting works has been published (e.g. Cavinato 2004; Christopher and Peck 2004; Jüttner 2005; Kleindorfer and Saad 2005; Malone 2006; Natarajathinam et al. 2009; Peck 2003, 2006; Sheffi and Rice 2005; Stemmler 2006; Svensson 2000; Waters 2007). The common denominator of these works can be, in our opinion, a *process continuity oriented approach*. This approach has been the subject of several our works (e.g. Bukowski 2014, 2016; Bukowski and Feliks 2012, 2014; Bukowski et al. 2015, 2016), in which we proposed the following basic definitions of the main terms:

- *Continuity*—a system capability to deliver products or services at acceptable, predefined performance level under the real work conditions (e.g. despite disruptive events *DE*).
- *Disruptive event (DE)*—an act of delaying or interrupting the process continuity (e.g. system failure, natural catastrophe, man-made fault).
- *Vulnerability to a disruptive event (V)*—the degree to which a system is affected by a disruptive event.

- *Vulnerability metric*—the disruption impact described by two main indicators: the expected loss of performance (L_D), and disruption time (T_D).
- *Resilience to a disruptive event (RES)*—the ability of a system to absorb and withstand the disruption impact, and still continue to deliver products or services at acceptable predefined performance level, as well as the adapt-capacity to a new work conditions.
- *Resilience metric*—a collective term described by the three main indicators: absorbability (*ABS*), recoverability (*REC*), and adaptability (*ADA*).

Based on these assumptions we proposed *the concept of disruption tolerant operation* (see Sect. 4.3.2). This concept is based on the process oriented approach and is closely related to the ideas of resilient enterprise (Sheffi 2007) as well as business continuity management (British Standards Institute 2006). The model is based on a typical course of a service delivery process, interrupted by an occurrence of a disruptive event leading to a disruption of this process continuity (general model shown in Fig. 4.4). A quantitative interpretation of this model is shown in Fig. 6.7. The thick line shows the course of an idealized system operation as it changes its performance in function of time. Prior to the occurrence of a disruptive event the system was functioning at the recommended level of performance. The occurrence of a disruptive event is immediately followed by a sharp decline in system performance, until it reaches a minimum level of performance higher than a critical level of performance ($P_{Min} > P_{Cri}$). With the capacity to absorb the effects of a disruptive event, the system maintains its basic functions and gradually increases its performance. After the time t_4 , it achieves a recovered performance level, which lies above the acceptable level of performance ($P_{Rec} > P_{Acc}$). The final phase of the

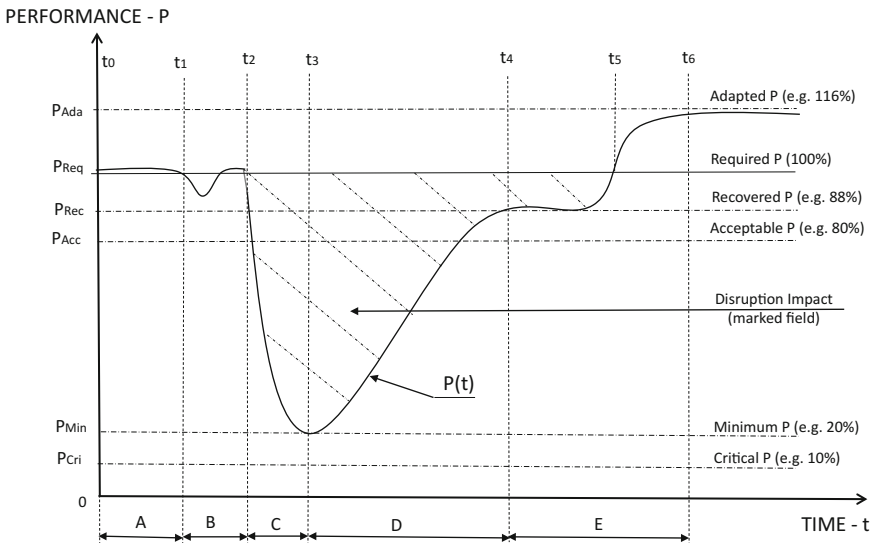


Fig. 6.7 Typical course of a product delivery process with a continuity disruption

course is characterized by the ability to adapt to new conditions, and as a result the system performance improves.

Generally, there can be distinguished the following five fundamental phases in a typical course of a service delivery process with a continuity disruption (Fig. 6.7):

- A Resistant state—characterized by no reaction to small disturbances,
- B Robust behavior—with short-term loss of performance after a disturbance and rapid return to the required state,
- C Absorption phase (*ABS*)—distinguished by ‘coping’ with disruption and continuity retain of operation,
- D Recovery phase (*REC*)—characterized by ‘bounce back’ to acceptable performance level,
- E Adaptation phase (*ADA*)—distinguished by ‘learning’ from disruption and transformation to the new work conditions.

The vulnerability and resilience properties appear in the C, D, and E phases, so the disruption curve shape will be the basis for a quantitative evaluation of these properties. As shown in Fig. 6.7, the loss of performance is proportional to the area between the line showing the required performance and the actual course of the performance. Therefore, the general metric for vulnerability can be described by two-dimensional variable (duplet):

$$V = \langle L_D, T_D \rangle \quad (6.5)$$

where:

disruption impact

$$L_D = \int_{t_2}^{t_5} [P_{Req} - P(t)] dt \quad (6.6)$$

disruption time

$$T_D = t_5 - t_2 \quad (6.7)$$

P_{Req} required performance level,

$P(t)$ performance at the time t ,

t_2 beginning of disruption,

t_5 end of disruption.

Resilience metrics is represented as a collective term described by three dimensional vector as follows:

$$RES = \langle ABS, REC, ADA \rangle \quad (6.8)$$

where:

$$ABS = \frac{P_{Min}}{P_{Req}} \quad (6.9)$$

$$REC = \frac{P_{REC}}{P_{Req}} \quad (6.10)$$

$$ADA = \frac{P_{ADA}}{P_{Req}} \quad (6.11)$$

6.2.3.2 Research Subject

The subject of research was a steel mill located in Central Europe (Bukowski et al. 2015, 2016). The plant is supplied with large amount of raw material required for a production, of which the strategic one is an iron ore (in the amount of approx. 5.5 million tonnes per year). The materials essential for a production process are being delivered to the stockpile buffer, which is characterized by a limited warehouse space. The capacity of the stockpile determines the maximum possible level of the reserve volume. Due to the significant collection and storage costs of resources in an investigated steel mill, the limit of the volume of the stock, has been set, which after assuming the regular supply of iron ore, should ensure the continuity of the production process. Iron ore is imported from abroad—from East Europe (railway transport) and Brazil (combined transport). In the investigated company iron ore is mainly delivered from Ukraine. It can also be delivered from Serbia, however the supply from this country is carried out only from time to time. From Ukraine ore is transported to Poland directly by railway carriages. Depending on the distance between the mine and Polish border as well as the weather conditions, the delivery time, i.e. the entry of a train into the steelworks area, varies from 2 up to 5 days. The delivery can be realized in different ways depending on the current conditions. Typically, supplier A (Ukraine) covers 80% of the demand for raw materials, while the remaining 20% provides supplier B (Brazil). In case of supply disruptions from two of the above mentioned suppliers, the demand for raw materials may be covered by the delivery from a supplier C (Serbia), but this involves higher transport costs and longer time of delivery.

Timely delivery depends on many factors which are often unpredictable. For example, the transport processes can be disrupted by breakdowns in the means of transport, or (in winter) inability to discharge the cargo due to its freezing. Such cases cause the discontinuity of supplies whose effects may be different, even including the production stoppage.

6.2.3.3 Research Methodology

In order to investigate the effect of such disturbances on the continuity of production process, the simplified simulation model of the raw materials supply network was constructed. We used the demo version of the software AnyLogic (AnyLogic Simulation Software 2015) which allows to connect different techniques of the system modelling. These techniques include: the continuous simulation using the method of system dynamics modelling (SDM), discrete event simulation (DES) and agent-based modelling (ABM). System dynamics method allows to model the structure and dynamics of complex systems and processes occurring within them. It takes into account the feedback systems that describe cause-effect reaction between the elements of the system under research. The fundamental premise of this method is to consider the system as a coherent unity in terms of its behaviour. The basic elements used to describe the behaviour of the system are: Stocks, Flows and Information.

Typical business activities include one or more of the following five types of stocks: materials, personal, capital equipment, orders, and money. The most visible signs of the operation of a process are often movements of these five types of stocks, and these are defined as follows:

- **Materials.** This type includes all stocks and flows of physical goods which are part of a production and distribution process, whether raw materials, in-process inventories, or finished products.
- **Personnel.** This type of stocks generally refers to actual people, as opposed, for example, to hours of labor.
- **Capital equipment.** It includes such things as factory space, tools, and other equipment necessary for the production of goods and provision of services.
- **Orders.** They include such things as orders for goods, requisitions for new employees, and contracts for new space or capital equipment. Orders are typically the result of some management decision which has been made, but not yet converted into the desired result.
- **Money.** This type of stocks is used in the cash sense. That is, a flow of money is the actual transmittal of payments between different stocks of money.

Stocks define static part of the system. Flows define how values of stocks change in time and thus define the dynamics of the system.

The modelling of dynamic processes using system dynamics methods carries with it some restrictions, e.g. resulting from the difficulties in taking into account the occurrence of the disturbances within logistics networks. Disruptions often have random nature, belong to rare events and have a significant impact on the efficient functioning of any system, especially on its operational level. To allow inclusion of such a type of cases one should combine dynamics system modelling with discrete system simulation and agent-based modelling techniques. An intelligent agent is a computer software or device that works on its own in an open, distributed environment, and solves a problem or perform a specific task (Swaminathan et al. 1998).

The agent perceives its environment and may interact with it, it is also characterized by the autonomy (it can operate without human involvement or other agent). Nowadays applications are more and more often are based on multi-agent systems, i.e. a loosely affiliated networks of agents, which operate to solve the problems that lie beyond their individual capabilities and scope of knowledge. The advantage of this approach is the speed of obtaining results (each of the agents has to solve the problem of lesser complexity) and the use of a wider range of knowledge when making the final decision (knowledge of many agents).

The model presented below combines the three mentioned above ways of modelling. The main part of the model, reflecting the realization of supply chain and shown schematically in Fig. 6.7 was built from the elements used in the modelling of dynamic processes. The model takes into account the relevant logistic delays. The risks arising from the disruption within a supply chain and the ways of preventing their adverse effects were modelled using agent systems, while the moments, when threats occur were modelled as random discrete events with the use of the corresponding distributions. The task of the agents is an appropriate (not too early but also not too late) response to the presence of distortions within the supply cycle in order to sustain continuity of a production by providing the required amount of raw materials to the plant. The expert team identified 15 of the most important scenarios for disruptive events which have been analysed using computer simulation (Table 6.8). In addition, the following options were analysed for each scenario:

Table 6.8 The scenarios for disruptive events

Scenario	Before disruption (% of delivery)			After disruption (% of delivery)		
	Sup. A (%)	Sup. B (%)	Sup. C	Sup. A	Sup. B (%)	Sup. C
S1	80	20	None	None	20	80%
S2	80	20	None	None	100	None
S3	80	20	None	None	40	60%
S4	80	20	None	None	20	None
S5	60	40	None	None	40	60%
S6	60	40	None	None	100	None
S7	60	40	None	None	60	40%
S8	60	40	None	None	40	None
S9	50	50	None	None	50	50%
S10	50	50	None	None	100	None
S11	50	50	None	None	70	30%
S12	50	50	None	None	50	None
S13	20	80	None	None	80	20%
S14	20	80	None	None	100	None
S15	20	80	None	None	80	None

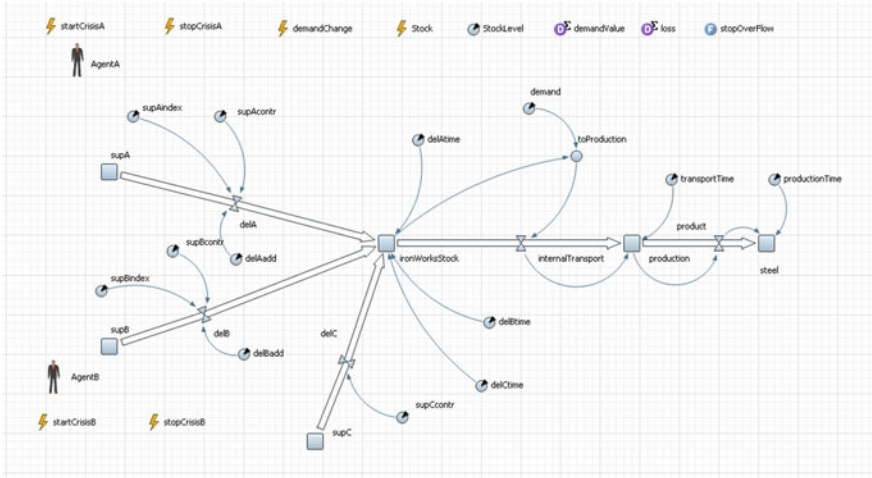


Fig. 6.8 The simulation model of the logistics network supply system for a steel mill

- I. no resources in the stockpile ('lean' strategy—Just In Time supplying)
- II. resources in the stockpile covering the five-days production (sustainable safe strategy)
- III. resources in the stockpile covering the ten-days production ('crisis' strategy).

It should be noted that in the absence of any distortions the realization of the option I is the cheapest one, but in the event of a major supply disruption, it leads to a complete stoppage of a production (which, in case of steel industry, results in enormous losses).

The break in the supply of raw material may be:

- a. short—up to 5 days,
- b. average—up to 10 days,
- c. long—up to 15 days.

The assumed delivery time for groups of individual suppliers are as follows: supplier A—2 days, supplier B—10 days and supplier C—3 days. In all cases the assumptive value of demand was constant. Based on the model shown in Fig. 6.8 there were carried out 1000 simulation experiments for each case. The results of these simulations are shown in Table 6.9 providing the percentage production loss for specific scenarios designated for the quarter (3 months) of a year, as a practical measure of the system vulnerability to the disruptive events.

Table 6.9 The percentage of production loss for each scenario

Scenario	I a	I b	I c	II a	II b	II c	III a	III b	III c
S1	3.56	5.92	5.92	0	0.39	0.39	0	0	0
S2	3.56	7.98	11.78	0	2.43	6.23	0	0	0.74
S3	3.56	6.43	7.30	0	0.88	1.75	0	0	0
S4	3.56	8.00	12.46	0	2.45	6.90	0	0	1.34
S5	2.67	3.99	3.99	0	0	0	0	0	0
S6	2.67	5.97	8.56	0	0.43	3.01	0	0	0
S7	2.67	4.64	5.47	0	0	0	0	0	0
S8	2.67	6.00	9.33	0	0.45	3.78	0	0	0
S9	2.22	3.32	3.32	0	0	0	0	0	0
S10	2.22	4.98	7.10	0	0	1.55	0	0	0
S11	2.22	3.98	4.83	0	0	0	0	0	0
S12	2.22	5.00	7.78	0	0	2.22	0	0	0
S13	0.89	1.33	1.33	0	0	0	0	0	0
S14	0.89	1.99	2.77	0	0	0	0	0	0
S15	0.89	1.99	2.89	0	0	0	0	0	0

6.2.3.4 Research Results

For the better visualization of the production losses it was assumed that during the ‘normal’ operation the production level corresponds to the level of the orders, but during the crisis the level of production may be lower, due to the lack of raw materials. Below, there is presented the exemplary scenario description and the results of a simulation for the case in which the break in supplies A lasts 14 days. The operation of the agent system aiming to maintain production ‘sets off’ additional deliveries in the proportion of: supplier B—40% and supplier C—60% of the demand for raw materials. This scenario, shown in Fig. 6.9a, illustrates an adverse situation because it additionally assumes the lack of any reserve on the stockpile (scenario S3-Ic). After 70 days a break in delivering from supplier A begins (black continuous line). In the fifth day of the crisis, the delivery from the Supplier B (green ‘triangle’ line) is increased from 20 up to 40% and the delivery from the Supplier C (yellow ‘point’ line) starts in the amount of 60% of the total demand for raw materials. Extra deliveries provide 100% production demand during the crisis and return to ‘normal’ levels (supplier A—80%, supplier B—20%, supplier C—0%) after the crisis stops.

In Fig. 6.9b the level of production and demand for a completed product is presented. As a result of the crisis the production drops down to about 20% (in the beginning of the crisis only regular deliveries from Supplier B are being provided), however, after several days the production level rises—first up to the level of 80% (after about 8 days, extra supplies from supplier C arrived) and then, after about 15 days, to the level of 100% (increased delivery from Supplier B also enters the steel mill). In Fig. 6.9c the percentage loss of production calculated per quarter is

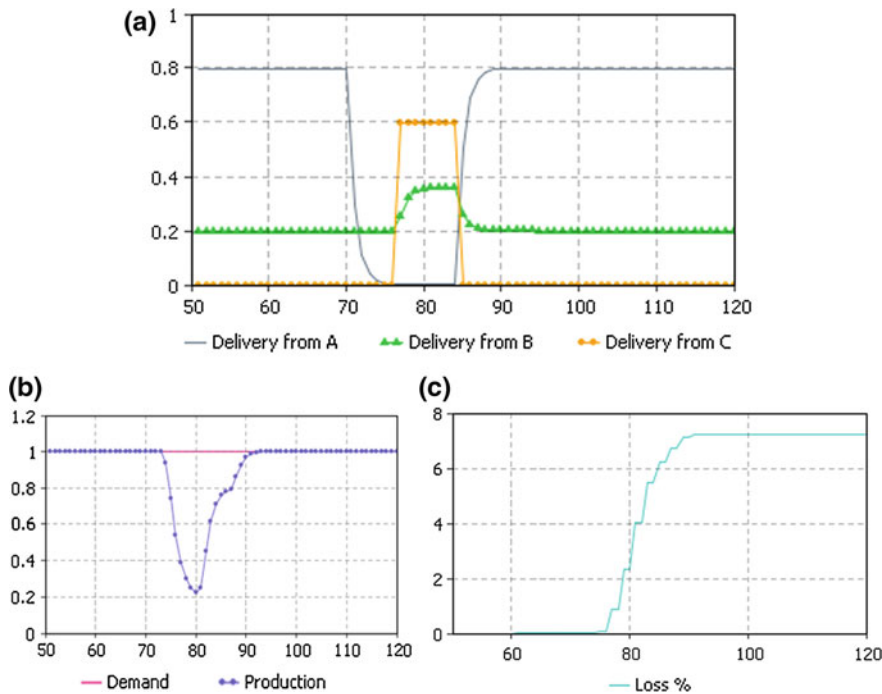


Fig. 6.9 Simulation results for the scenario S3-Ic: **a** the percentages of supplies for A, B, C suppliers; **b** production and demand level; **c** the percentage loss of production calculated per quarter

shown. The losses appear about a day of 75 and grow for about 15 days. The total production loss in relation to the demand for a completed product is 7.3%. Thus, the vulnerability measure of the tested system in this case (scenario S3-Ic) reaches the value $V = \langle 7.3\%; 15 \text{ days} \rangle$.

The same simulation tests were carried out for all scenarios and for all possible combinations I, II, III, a, b and c. The results of these tests are shown in Table 6.9 in the shortened form, and may serve as a preliminary assessment of the tested system vulnerability to threats resulting from individual risky scenarios. According to the assumptions presented in this model the agent actions are restricted, and oriented primarily at preventing production losses or their reduction to a minimum.

References

- AnyLogic Simulation Software (2015). <http://www.anylogic.com/features>. Access 15 Nov 2015
- AIAG (2008) Potential failure mode and effects analysis (FMEA) 4th edn. Reprinted from Potential failure mode and effects analysis (FMEA), 4th edn, 2008. Manual with permission of Chrysler, Ford and GM Supplier Quality Requirements Task Force. <http://onlinelibrary.wiley.com/doi/10.1002/9781118312575.app1/pdf>. Access 22 July 2017
- AMBER (2009) Assessing, measuring, and benchmarking resilience, FP7 – 216295
- Aven T (2011) On some recent definitions and analysis frameworks for risk, vulnerability and resilience. *Risk Anal* 31(4):515–522
- Aven T (2014) A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliab Eng Syst Saf* 121:1–10
- Aven T, Baraldi P, Flage R, Zio E (2014) Uncertainty in risk assessment. Wiley, New York
- Boran FE, Genc S, Kurt M, Akay D (2009) A multi-criteria intuitionistic fuzzy group decision making for supplier selection with TOPSIS method, *Expert Systems with Applications*, 36 (2009) 1136311368
- British Standards Institute (2006) PAS 56: Guide to business continuity management. BSI, London
- Bross ME, Zhao G (2004) Supplier selection process in emerging markets—The case study of Volvo Bus Corporation in China, School of Economics and Commercial Law Göteborg University
- Bukowski L (2014) Managing disruption risks in the global supply networks—a trans-disciplinary approach. In: *Proceedings of international conference on industrial logistics*, Croatia, pp 101–106
- Bukowski L (2016) System of systems dependability—theoretical models and applications examples. *Reliab Eng Syst Saf* 151(2016):76–92
- Bukowski L, Feliks J (2005) Application of fuzzy sets in evaluation of failure likelihood. In: *Proceedings of the 18-th international conference on systems engineering—Las Vegas 2005*, IEEE CS, pp 170–176
- Bukowski L, Feliks J (2012) Multi-dimensional concept of supply chain resilience. In: *Proceedings of the 2nd Carpathian logistics congress*, Jesienik
- Bukowski L, Feliks J (2014) A unified model of systems dependability and process continuity for complex supply chains. In: *Safety and reliability: methodology and applications*. Taylor & Francis Group, A Balkema Book, London, pp 2395–2403
- Bukowski L, Feliks J, Majewska K (2015) Modelling and simulation of disruption risk in the complex logistic networks—a multimethod approach. In: *Safety and reliability of complex engineered systems*. Taylor & Francis Group, A Balkema Book, London, pp 3911–3918
- Bukowski L, Feliks J, Majewska K (2016) Logistic system resilience modelling—a dynamic, multiagent, service engineering oriented approach. In: *Risk, reliability and safety: In-novating theory and practice*. Taylor & Francis Group, A Balkema Book, London, pp 2207–2214
- Cavinato JL (2004) Supply chain logistics risks. *Int J Phys Distrib Logist Manag* 34(5):383–387
- Chen-Tung C, Ching-Tornng L (2006) A fuzzy approach for supplier evaluation and selection in supply chain management. *Prod Econ* 102(2006):289–301
- Christopher M, Peck H (2004) Building the resilient supply chain. *Int J Logist Manag* 15(2), 1–13
- Chuan WL (2009) Supplier selection under uncertainty: a switching option perspective. *Ind Manag Data Syst* 1092:191–205
- D’Inverno M, Luck M (2004) Understanding agent systems. Springer, Berlin
- De Boer L, Van der Wegen L, Telgen J (1998) Outranking methods in support of supplier selection. *Eur J Purch Supply Manag* 4(2/3), 109–118 (1998)
- Degraeve Z, Roodhooft F (1999) Effectively selecting suppliers using total cost of ownership. *J Supply Chain Manag* 35(1), 5–10 (1999)
- Degraeve Z, Labro E, Roodhooft F (2000) An evaluation of supplier selection methods from a Total Cost of Ownership perspective. *Eur J Oper Res* 125(1):34–59

- Dekker S et al (2008) Resilience engineering: new directions for measuring and maintaining safety in complex systems. Final Report December 2008
- Dong C (2007) Failure mode and effects analysis based on fuzzy utility cost estimation. *Int J Qual Reliab Manag* 24(9), 958–971
- Dulmin R, Mininno V (2003) Supplier selection using a multi-criteria decision aid method. *J Purch Supply Manag* 9(4):177–187
- Elanchezhian C, Ramnath VB, Kesavan R (2010) Vendor evaluation using multi criteria decision making. *Int J Comput Appl* 5(9):0975–8887
- Faez F, Ghodsypour SH, O'Brien C (2009) Vendor selection and order allocation using an integrated fuzzy case-based reasoning and mathematical programming model. *Int J Prod Econ* 121(2):395–408
- Geum Y, Cho Y, Park Y (2011) A systematic approach for diagnosing service failure: Service-specific FMEA and grey relational analysis approach. *Math Comput Model* 54 (2011):3126–3142
- Ghodsypour SH, O'Brien C (1998) A decision support system for supplier selection using an integrated analytic hierarchy approach and linear programming. *Int J Prod Econ* 56/57:199–212 (1998)
- Gonzalez ME, Quesada G, Monge CAM (2004) Determining the importance of the supplier selection process in manufacturing: a case study. *Int J Phys Distrib Logist Manag* 34(6):492–504
- Guidelines for making PFMEA. <https://daimler.portal.covisint.com/web/india/downloads>. Access 22 July 2017
- Hartley RVL (1928) Transmission of information. *Bell System Tech. J.* 7(3):535–563
- Hill RP, Nydick RL (1992) Using the analytic hierarchy process to structure the supplier selection procedure. *Int J Purch Mater Manag* 28(2):31–36
- Hinkle CL, Robinson PJ, Green PE (1969) Vendor evaluation using cluster analysis. *J Purch* 5 (3):49–58
- Ho W, Xu X, Dey PK (2010) Multi criteria decision making approaches for supplier evaluation and selection: a literature review. *Eur J Oper Res* 202(1):16–24
- Hollnagel E, Woods DW, Leveson N (eds) (2006) Resilience engineering: concepts and precepts. Ashgate
- Humphreys PK, Wong YK, Chan FTS (2003) Integrating environmental criteria into the supplier selection process. *J Mater Process Technol* 138(1–3):349–356
- IATF 16949 (2016) Automotive quality management system standard
- ISO 9000:2015, Quality management systems—fundamentals and vocabulary (2015)
- ISO 9001:2015, Quality management systems—requirements (2015)
- Jüttner U (2005) Supply chain risk management. *Int J Logist Manag* 16(1):120–141
- Kleindorfer PR, Saad GH (2005) Managing disruption risks in supply chains. *Prod Oper Manag* 14 (1):53–68
- Kroger W, Zio E (2011) Vulnerable systems. Springer, London
- Kuo RJ, Wang YC, Tien FC (2010) Integration of artificial neural network and MADA methods for green supplier selection. *J Cleaner Prod* 18(12):1161–1170
- Lee EK, Ha S, Kim SK (2001) Supplier selection and management system considering relationships in supply chain management. *IEEE Trans Eng Manag* 47(4):307–318
- Li CC, Fun YP (1997) A new measure for supplier performance evaluation. *IIE Trans* 29(1):753–758
- Liu FHF, Hai HL (2005) The voting analytic hierarchy process method for selecting supplier. *Int J Prod Econ* 97(3):308–317
- Maggie CYT, Tummala VMR (2001) An application of the AHP in vendor selection of a telecommunications system. *Omega* 29(2001):171–182
- Malone R (2006) Growing supply chain risks. www.Forbes.com
- Min H (1994) International supplier selection: a multi-attribute utility approach. *Int J Phys Distrib Logist Manag* 24(5):24–33

- Natarajarathinam M et al (2009) Managing supply chains in times of crisis: a review of literature and insights. *Int J Phys Distrib Logist Manag* 39(2009):535–573
- Pearson JM, Ellram LM (1995) Supplier selection and evaluation in small versus large electronics firms. *J Small Bus Manag* 33(4):53–65
- Peck H (2003) Creating resilient supply chains: a practical guide. School of Management, Cranfield University, Cranfield, Bedford
- Peck H (2006) Supply chain vulnerability, risk and resilience. In: D Waters D (ed) *Global logistics*, 5th edn. Kogan Page, London
- Saaty TL, Vargas LG (2006) Decision-making with the analytic network process economic, political, social and technological applications with benefits, opportunities, costs and risks. Springer, New York
- Sampson SE (2010) A unified service theory. In: Salvendy G, Karwowski W (eds) *Introduction to service engineering*. Wiley, New Jersey
- Sanayei A, Mousavi SF, Abdi MR, Mohaghar A (2008) An integrated group decision-making process for supplier selection and order allocation using multi-attribute utility theory and linear programming. *J Franklin Inst* 345(2008):731–747
- Sanchis R, Poler R, Lario FC (2012) Identification and analysis of disruptions: the first step to understand and measure enterprise resilience. In: 6th international conference on industrial engineering and industrial management, Vigo, July 18–20
- Scarborough J (2007) Risks during transportation. RPW Reports, London
- Security Service (2006) Security advice: business continuity. HMSO, London (www.mi5.gov.uk)
- SEF (2001) Systems engineering fundamentals. https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf
- Sharland A, Eltantawy RA, Giunipero LC (2003) The impact of cycle time on supplier selection and subsequent performance outcomes. *J Supply Chain Manag Glob Rev Purch Supply* 39(3)
- Sheffi Y (2007) The resilient enterprise: overcoming vulnerability for competitive advantage, MIT Press
- Sheffi Y, Rice JB Jr (2005) A supply chain view of the resilient enterprise. *MIT Sloan Manag Rev* 47:41–48
- Shyur HJ, Shih HS (2006) A hybrid MCDM model for strategic vendor selection. *Math Comput Model* 44(2006):749–761
- Stemmler L (2006) Risk in the supply chain. In: Waters D (ed) *Global logistics*, 5th edn. Kogan Page, London
- Svensson G (2000) Conceptual framework for the analysis of vulnerability in supply chains. *Int J Phys Distrib Logist Manag* 30:731–749
- Svensson G (2004) Supplier segmentation in the automotive industry: a dyadic approach of a managerial mode. *Int J Phys Distrib Logist Manag* 34(1/2):12–38
- Swaminathan J, Smith S, Sadeh N (1998) Modelling supply chain dynamics: a multiagent approach. *Decis Sci* 29(3)
- Tahriri F, Osman MR, Ali A, Yusuff RM (2008) A review of supplier selection methods in manufacturing industries. *Suranaree J Sci Technol* 15(3):201–208

- Torfi F, Farahani RZ, Rezapour S (2010) Fuzzy AHP to determine the relative weights of evaluation criteria and fuzzy TOPSIS to rank the alternative. *Appl Soft Comput* 10:520–528
- Waters D. (2007) *Supply chain risk management: vulnerability and resilience in logistics*. Kogan Page Limited, London & Philadelphia
- Weber CA, Ellram LM (1992) Supplier selection using multi-objective programming: a decision support system approach. *Int J Phys Distrib Logist Manag* 23(2):3–14
- Weber CA, Current JR, Benton WC (1991) Vendor selection criteria and methods. *Eur J Oper Res* 50(1991):2–18
- Weber CA, Current JR, Desai A (1998) Non-cooperative negotiation strategies for vendor selection. *Eur J Oper Res* 108(1998):208–223
- Welborn C (2010) Applying failure mode and effects analysis to supplier selection. *IUP J Supply Chain Manag* VII(3):7–14

Conclusions and Concluding Considerations

The subject of this book is to synthesise current knowledge in the field of designing, testing and evaluation of logistic networks subjected to disturbances and disruptions from a variable and uncertain environment, and on this background to present a new concept of dependable product delivery assurance. The challenges facing modern logistics result from the trends in the development of new technologies, especially information and communication technologies (e.g. Internet of Things), as well as from the current state of the global economy, which is still in the phase of dynamic changes. Therefore, the improvement of quality and competitiveness in the scope of logistic services requires continuous improvement of logistics infrastructures reliability and resilience as well as logistics processes effectiveness and efficiency, with particular emphasis on risk aspects including safety and security requirements.

In order to meet these challenges, the only practical approach is insufficient, as was the case in the earlier phases of logistics development, but also support based on scientific methods is needed. We propose define the term *Logistics* as a trans-disciplinary field of scientific knowledge concerning effective and efficient implementation of flows (movement and storage) of tangible and intangible assets (goods, persons, transactions, and related information) within systems composed of enterprises, their clients and other stakeholders. The Logistics understood in this way is based on three following *paradigms*:

- (a) *Network paradigm*. The subject of research are *logistic networks (LN)* understood as open engineered system of systems composed of interconnected logistic systems, operating under a strong influence of the environment, with which relations have a relevant influence on their behaviour. In practice a logistics network is a network organization consisting of *logistic infrastructure* and *logistic processes* implemented within it. A special case of the logistics network is the *supply chain (SC)*, which is characterized by the central coordination of flows as well as the integration of suppliers and recipients initiated by the dominant entity of the organization.

(b) *Flow paradigm* characterized by:

- Comprehensive (big-picture) approach,
- Dynamic-related methodology,
- Continuity-oriented view,
- Service-dominant logic,
- Customer-centric market-driven concept.

In modern, so-called *demand driven supply chains*, flows are in direct response to a single point of demand, and all components across a logistics network are synchronized to meet the demand that it is trying to fulfil (an example for such pull system is the Just in Time—Kanban process). A necessary element of logistics networks are systems that provide them with full *traceability*. It depends on the identification of goods and materials flows, used in manufacturing or processing, to enable the relevant production batch and material source to be traced in case of subsequent failures or complaint.

(c) *Transdisciplinary paradigm*. Transdisciplinarity is the way of scientific knowledge development which consists in viewing a phenomenon outside the boundaries of a single scientific discipline. Research methods come from various scientific disciplines and are applied in an iterative manner. In the case of logistics, these various disciplines are engineering, economics, management and social sciences. A comprehensive and holistic understanding of logistics requires simultaneous consideration of the network and flow paradigm, which is possible only from the transdisciplinary perspective.

Based on the above paradigms we propose the framework for evaluation of logistic networks operational risk and dependability (ELNORD), which has been divided into 10 steps. Step 1 concerns defining the problem. Typical problems are to design a new logistics network or modify an existing one for specific requirements and restrictions. The main inputs to the problem defining process include the customer's requirements and the project constraints. Requirements relate directly to the attributes of the system being designed, e.g. performance characteristics and operability related measures (see Sect. 3.3). They contain the stated life-cycle customer needs and objectives for the system, and they relate to quality of the system operation in its intended environment. Constraints are conditions that exist because of limitations imposed by the environment, available resources, or technology. This process's primary purpose is to transform the requirements into designs within the given constraints.

The goal of the second step is knowledge capturing. The general model of knowledge creating process is shown in Fig. 2.3. The entire process is presented as a chain of operations and flows that are subjected to disturbances. The raw data stored in Data Acquisition block is sent to the Data Processing block and subjected to the preparation process. The processed data flows to Data Verification block where they are verified for their veracity and then sent to Data Forming block for generation of Data Mining and Fusion of Data. Raw information flows to Information Evaluating block, where they are evaluated for their utility value and selected on this basis. The selected information is used in Building Patterns block to

search for relationships between individual pieces of information and build logical patterns, based on which a new knowledge is generated in New Knowledge Creation block. The last stage of the chain is to enrich the existing knowledge base with new knowledge and to create initial knowledge for further acquisition of new data. Section 2.1 contains more detailed analysis of capturing knowledge process with special stress on uncertainty of data and information as well as imperfection of the available knowledge.

Step 3 include the knowledge maturity assessment. Assessment of the *knowledge maturity* should be based on three basic criteria, namely: data veracity value (five levels), information utility value (five levels) and knowledge processing quality (five levels). Methods for determining these criteria are described in Sects. 2.1.2 and 2.1.3. The whole process of assessing the maturity of knowledge based on imperfect data, information and knowledge processing can be presented in the form of the following algorithm:

- Data Veracity evaluation;
- Information Utility evaluation;
- Knowledge Processing Quality evaluation;
- Knowledge Maturity assessment.

Comprehensive risk analysis is the subject of the fourth step. It should include all three basic groups of risks, namely: opportunity related risks (covering the risk of lost and missed chances), hazard related risks (including risks in a safety context), and threat related risks (concerning risks of detriment). This last group contains economic risk (the potential of losing something of value such as financial wealth, e.g. financial, commercial and price risks) as well as technical risk (operational risk—risk in context of operation system unavailability, e.g. potential for realization of unwanted scenario leading to a disruptive event with possibility of negative consequences). The basis for conducting such a risk analysis is Chap. 2, and especially Sects. 2.2 and 2.3 of this book.

Step 5 include the system describing. A full description of the assessed system should be carried out both in terms of system and process approach using both topology- and flow-based methodology (see Chap. 3). The infrastructure description should take into account its complexity and dependencies between elements of the structure, especially in the case of global supply networks. On the other hand, the process approach should be based on the service engineering principles to describe the specificity of the delivery processes (supply, demand and distribution) as accurately as possible. A quantitative description of the system should contain both performance and operationality related measures.

System designing is the subject of the step 6. Designing complex engineered system for the risky environment is a comprehensive process including two main stages, namely creating reliable system's infrastructure and process continuity assurance. In case of logistics networks, architecting of reliable engineered system of systems can be based on the principle of High Reliability Organisations, whereas the process continuity ensuring is usually based on the concept of Resilient Enterprise. A detailed describing of the system designing process can be found in Chap. 4 (Sects. 4.1 and 4.2).

Step 7 include the system modelling process. Modelling of logistics networks is divided into four main stages: modelling of logistic infrastructures using an agent based approach, modelling of logistic processes applying a dynamic based approach, modelling of demand variation using a probabilistic approach, and modelling of disturbances with an event driven approach. All these processes are described in Chap. 5.

Step 8—Simulation tests. The developed and verified model in step 7 is the starting point for the application phase, which consists in conducting simulation tests. The basis for simulation procedures is provided in Sect. 5.1, while specific solutions for logistics networks are presented in Sects. 5.2–5.5.

Risk and dependability evaluation are the subjects of the step 9. The evaluation of operational risk and dependability for complex engineered systems is a process that can be represented in the form of the general algorithm presented in Fig. 4.6. The method is implemented in 10 stages. The final stage of the proposed procedure is to assess the overall risk matrix, taking into consideration all potential risky scenarios as a consequence of the possible disruptive events. The entire disruption risk matrix will be expressed as a N-dimensional vector, where N is the number of investigated scenarios. The dependability measure of the system under consideration can be expressed by formula (4.3) interpreted as the likelihood to avoid disruptions that are more probable and more severe in consequences than it is acceptable for each possible risky scenario.

The last step No. 10 include the acceptance decision. The basis for decision-making about accepting or rejecting the solution are the results obtained in step 9. If the level of operational risk and dependability measure (determined as a result of simulation tests) are acceptable, it can be assumed that the logistics network is sufficiently well protected from threats and hazards. If, however, the test results are not satisfactory, then you should go back to step 6 and make changes to the system design, and then perform further research (steps 7–10) for the changed configuration of the logistics network. This procedure should be repeated until we receive fully satisfactory results.

As examples of the framework for evaluation of logistic networks operational risk and dependability application tree different cases are presented. First example concerns a modified PFMEA method as representative of a risk-oriented static approach. Next example is an expert system with fuzzy reasoning based on a process-continuity oriented approach. Last one uses a vulnerability related dynamic approach to create an expert system with agent-based simulation.

Summarizing, this book focuses on the technical aspects of risk and does not take full account of the human factors, such as the subjective perception of risk. It can be the cause of significant errors in the risk assessment, especially in cases of complex and interrelated threats and hazards as well as contradictory, ambiguous and conflicting information. Therefore, our further work will focus on expanding the area of research to include the cognitive perspective, that is issues related to risk psychology.

Appendix

Terminology

<i>Activity</i>	An intentionally designed and implemented action. We divide activities into operations, tasks and decisions.
<i>Act of a system</i>	An event that occurs without external stimuli as a self-determined action caused by the system itself.
<i>Adaptability</i>	Ability to adapt to changed working conditions (flexibility, agility, ability to learn).
<i>Availability</i>	Ability to be in state to perform the required functions under given work conditions. It is described by: reliability, maintainability and maintenance support performance.
<i>Background knowledge</i>	The ability to evaluate available information and understand reality in accordance with the current state of knowledge, including a judgment of the strength of this knowledge.
<i>Complexity</i>	A system feature conditioned by having many diverse and autonomous but interrelated and interdependent components or parts linked through many interconnections that do not allow the understanding or prediction of the system's behaviour on the basis of each component's behaviour.

<i>Confidentiality</i>	Unavailability to non-enabled persons.
<i>Consequences</i>	The effects of an activity with respect to the values defined (such as human life and health, environment and economic assets), covering the totality of states, events, barriers and outcomes, and often seen in relation to some reference values (planned values, objectives, etc.).
<i>Continuity</i>	A system capability to deliver products (services) at acceptable predefined performance level under the real work conditions (e.g. despite disruptive events).
<i>Damage</i>	Loss of resources (e.g. infrastructure).
<i>Dependability</i>	A collective term describing the time-related operating quality of a system.
<i>Dependability measure</i>	The likelihood to avoid disruptions that are more probable and more severe in consequences than it is acceptable for each possible risky scenario.
<i>Disruption risk</i>	Potential for realization of unwanted scenario leading to a disruptive event with possibility of negative consequences.
<i>Disruptive event</i>	An act of delaying or interrupting the process continuity (e.g. system failure, natural catastrophe, man-made fault).
<i>Disruptive event consequences</i>	Damage, harm, impact and severity.
<i>Disruptive risk metric</i>	The triplet (s_i, p_i, c_i) , where s_i is the i -th unwanted disruption scenario, p_i is the uncertainty measure (probability or possibility) of that scenario, and c_i is the severity measure (consequence) of the i -th scenario, for $i = 1, 2, 3, \dots, n$.
<i>Dynamic system (multi-state system)</i>	A system to which events occur, whose state changes overtime.

<i>Environment of a system</i>	A set of elements and their relevant properties, which are not part of the system (they are outside its borders) but may influence (substantially) the state of the system.
<i>Event</i>	The occurrence or change of a particular set of circumstances such as a system failure, an earthquake, an explosion or an outbreak of a pandemic.
<i>Events</i>	A change in the state of the system or its environment which can initiate the start of a process, interfere with it causing errors and pauses or end it when the desired outcome is achieved.
<i>Exposure</i>	Being subjected to a risk source.
<i>Extensibility</i>	The ability of an open system to add new components, subsystems or systems, as well as new capabilities to a system.
<i>Flexibility</i>	Means that a given system, depending on the current needs, can be reconfigured and modified to changing situations.
<i>Flows</i>	Relations that consist in the movement of goods (transport) and information (communication).
<i>Function of a system</i>	Generating results in line with the goals and objectives of the system, regardless of the state of the system and its environment.
<i>Functioning</i>	Understood as a manifestation of rational behaviour, involving the fulfilment of certain (required) functions, e.g. the execution of production processes or services. The purpose of an operational system should be to fulfil the expectations of the object of the action (owner, customer, society).
<i>Goal of an active system</i>	The preferred state of a system, guaranteeing the production of a given functions at the outcome

	within a specified, relatively short time period.
<i>Harm</i>	Physical or psychological injury or damage.
<i>Hazard</i>	A risk source where the potential consequences relate to safety application (e.g. harm).
<i>Impact</i>	The effect that the consequences have on specified values.
<i>Integrity</i>	Impossibility of introducing changes into the system by non-enabled persons.
<i>Integrateability</i>	Means that a given system is able to form, coordinate, or incorporate into a larger, functioning or unified whole.
<i>Interoperability</i>	The ability of connected, autonomous, flexible coupled and usually heterogeneous systems to cooperate and to exchange flows of data, services, material and energy to and/or from other systems, while continuing their own way of operation.
<i>Interchangeability</i>	Means that a given system or a part of it can be replaced with another one without losing the basic system properties.
<i>Likelihood</i>	A measure for expressing uncertainty, variation or beliefs, following the rules of probabilistic, possibilistic or veristic calculus.
<i>Logistics infrastructure</i>	A logistic system characterized primarily by structural and spatial complexity.
<i>Logistics</i>	A transdisciplinary field of scientific knowledge concerning effective and efficient implementation of flows (movement and storage) of tangible and intangible assets (goods, persons, transactions, and related information) within systems composed of enterprises, their clients and other stakeholders.

Logistics network

A network organization consisting of logistic infrastructure and logistic processes implemented within it.

Logistics process

A sequence of events and actions connected with mutual relationships of the type of flows, aimed at moving and storing material and non-material resources (goods, persons, transactions, and related information). Logistic processes are characterized above all by time extension.

Logistics system

A spatially complex structure, consisting of individual objects connected together (e.g. subsystems), characterized by certain permanent behaviours (e.g. fulfilled functions), within which specific logistic processes are implemented.

Maintainability

Ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance.

Maintenance support performance

Effectiveness of an organization in respect to maintenance support.

Modularity

Means that a given system (usually in order to improve its maintainability) is built of functional blocks, separating the system's capacities into modules.

Network organisation

A structurally, spatially and temporally complex process organisation, whose elements comprise of independent enterprises, and its properties are emergent in their nature.

Objective of an active system

The preferred state of the system, guaranteeing the production of a given function in an ultimately desirable degree in a long period of time (a long-term goal).

Operating quality

Multidimensional measure of system performance related to its effectiveness, efficiency and continuity.

<i>Organisation</i>	Separate (from its environment), controllable, function-producing and goal-seeking entirety, whose elements are connected by mutual relations, both physical and intangible.
<i>Portability</i>	The ability to be readily moved from one environment to another.
<i>Process</i>	A system whose elements are events and actions connected by flow relations. A process is a structured chain of events and actions interconnected by flow relations, the aim of which is to achieve the desired result.
<i>Purposefulness</i>	Pursuing a certain state which can be defined in a strategic and operational scale.
<i>Reaction of a system</i>	An event for which another event, preceding it, that occurs to the same system or its environment is necessary and sufficient.
<i>Recoverability</i>	Capacity of a system to recover from a failure (restoration), in the acceptable time and costs limits.
<i>Reliability</i>	Ability to perform the required functions, without failure, for a given time interval, under given work conditions.
<i>Replaceability</i>	Is understood as the ability of one system, component or person to take the place of another, especially as a substitute or successor.
<i>Resilience</i>	A collective term describing the ability of a system to absorb and withstand the disruption impact, and still continue to deliver products (services) at acceptable predefined performance level.
<i>Resilience metric</i>	A collective term described by the three main indicators: absorbability, recoverability, and adaptability.
<i>Resilience to a disruptive event</i>	The ability of a system to absorb and withstand the disruption impact, and still continue to deliver

Response of a system

products or services at acceptable predefined performance level, as well as the adapt-capacity to a new work conditions.

An event for which another event, preceding it, that occurs to the same system or to its environment is necessary but not sufficient.

Risk

The potential of gaining or losing something of value (such as physical health, social status or financial wealth) resulting as outcome from a given activity (planned or not planned) taken in spite of uncertainty.

Risk analysis

Systematic process to comprehend the nature of risk and to express the risk, with the available knowledge. It include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risks to individuals, public, organizations, and to society.

Risk appetite

Amount and type of risk an individual or an organisation is willing to take on risky activities in pursuit of values or interests.

Risk assessment

Systematic process to comprehend the nature of risk, express and evaluate risk, with the available knowledge.

Risk aversion

Disliking or avoiding risk.

Risk awareness

Having an understanding of the risk (e.g. the risk sources, the hazards and threats, the potential consequences).

Risk characterization

A qualitative and/or quantitative description of the risk; i.e., a structured statement of risk usually containing the elements: risk sources, causes, events, consequences, uncertainty measurements and the knowledge that the judgments are based on.

Risk communication

Exchange or sharing of risk-related data, information and knowledge between and among different target groups (such as regulators, stakeholders, consumers, media, general public).

Risk evaluation

Process of comparing the result of risk analysis against risk (and often benefit) criteria to determine the significance and acceptability of the risk.

Risk framing

The initial assessment of a risk problem, clarifying issues and defining the scope of subsequent work.

Risk governance

The application of governance principles to the identification, assessment, management and communication of risk. Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented.

Risk management

Activities to handle risk such as prevention, mitigation, adaptation or sharing. It often includes trade-offs between costs and benefits of risk reduction and choice of a level of tolerable risk.

Risk metric

The triplet (C', U', K) , where C' is a measure of some consequences C for a specific value V resulting as an outcome from a given activity A (e.g. positive or negative impact), U' represents a measure of uncertainty U associated with C' (e.g. probability or possibility), and K is the background knowledge that supports evaluation of C' and U' (including a judgment of the strength of this knowledge).

<i>Risk perception</i>	The subjective judgment people make about the risk, and may vary person to person.
<i>Risk source</i>	A factor or an agent which alone or in combination with other factors (agents) has the potential to give rise to some specified consequences.
<i>Robustness</i>	The ability of a system to resist change without adapting its initial stable configuration.
<i>Safety</i>	Ability to operate, normally or abnormally, without danger of causing human injury or death and without damage to the system's environment.
<i>Security</i>	Ability to prevent an unauthorized access to, or handling of system state.
<i>Severity</i>	The magnitude of the damage, harm or impact
<i>State of a system at t_i moment</i>	The set of relevant properties which the system has at that time. A set of system states may be infinite, but in extreme cases it can be reduced to two states important for the observer (e.g. suitable–unsuitable, moving–resting, meeting the requirements–not meeting the requirements).
<i>State of a system's environment at t_i moment</i>	A set of the relevant properties of its environment at that time.
<i>Static system (one-state system)</i>	One to which no events occur, therefore it is unchanging over time.
<i>Supply chain</i>	A special case of the logistics network characterized by central coordination of flows and the process of integration of suppliers and recipients initiated by the dominant entity of the organization.
<i>Survivability</i>	Capability of a system to fulfil its mission, in a timely manner, in the presence of disruptive events.

System

A set of interrelated elements. Thus a system is an entity which is composed of at least two elements and a relation that holds between each of its elements and at least one other element in the set. Each of a system's elements is connected to every other element, directly or indirectly. Furthermore, no subset of elements is unrelated to any other subset.

System of systems (SoS)

A set of systems that results when independent systems are integrated into a larger system that delivers unique capabilities.

System's behaviour

A sequential chain of changes to the system occurring as a result of antecedent events such as: reactions, responses and acts. These changes can therefore initiate other events in the system or its environment.

Tasks

Sequences of activities or operations performed by the same 'actor' on the same object, and

Threat

A risk source used in relation to reliability and security application (e.g. damage).

Uncertainty

A situation of having imperfect knowledge about the true value of a quantity or the future consequences of an activity, scenario or event.

Uncertainty metrics

A subjective probability (based on the background knowledge) or a possibility function.

Vulnerability

The degree to which a system is affected by a risk source or susceptible to damage, harm or impact.

Vulnerability metric

The disruption impact described by two main indicators: the expected loss of performance, and disruption time.

Vulnerability to a disruptive event

The degree to which a system is affected by a disruptive event.